Mr. Claude Doucet
Secretary General
Canadian Radio-television and Telecommunications Commission
Les Terrasses de la Chaudière
1 Promenade du Portage
Gatineau, Québec J8X 4B1

RE: ***Call for comments – Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety,*** **Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9, 13 January 2021: Intervention of the Canadian Internet Registration Authority**

15 March 2021

Dear Mr. Doucet,

1. The above-captioned call ("**CETNC 2021-9**" or the "**Notice**") seeks comments on 10 questions related to "guid[ing] development of a network-level blocking framework" that would "limit the harm caused to Canadians by botnets",[1] but would "need" to safeguard, "at a minimum",

   a) subscriber privacy, minimizing the "monitoring, collection and usage" of subscriber information;

   b) accountability, by ensuring lack of bias and alignment with Canadians' best interests.

   c) user choice, through opt-in and -out toggles; and

   d) accuracy, by addressing overblocking and false-positive correction.[2]

2. Like many stakeholders in the Canadian internet, the Canadian Internet Registration Authority ("**CIRA**") was surprised by the Notice. The Commission has not, in the past, established guidelines or convened proceeding in respect of baseline network security requirements nor taken up a recent recommendation to begin doing so.[3] Rather, such activities have for some time been convened under other auspices.[4]

3. The Notice does not disclose a particular catalyzing event or animating concern leading to its issuance at this time; the framework the Notice proposes does not correspond to a clear *Telecommunications Act*

---

1 Notice, paragraph 17

2 Notice, paragraph 15. We have re-ordered these categories in order to better correspond to the sequence of questions posed in the Notice. In addition, where paragraph 15 presents separately the role of safeguards to (i) "ensure Internet subscriber privacy" and to (v) "minimize subscriber information monitoring, collecting, and usage", we have combined these for simplicity, as they relate to substantially similar requirements.

3 Broadcasting and Telecommunications Legislative Review Panel (J. Yale, chair), *Canada's communications future: time to Act* (Ottawa, 2020) ("**Yale Report**"), recommendation 46 ("Canada should not wait to establish security baselines that enhance trust in telecommunications markets. We recommend that the CRTC initiate a proceeding to update the Security Best Practices for Canadian Telecommunications Service Providers issued by the Canadian Security Telecommunications Advisory Committee [("**CSTAC**")] and to determine to which classes of service providers these practices should apply.").

4 For example, CSTAC was established in 2010 within Industry Canada, and has maintained a list of security best practices for Canadians telecommunications service providers since 2013.

policy objective[5] or requirement of Canada's anti-spam legislation ("**CASL**") that the Commission must pursue. But the Commission's Department Plan, published for the 2021-22 year some five weeks after the Notice's issuance, does now includes the topic of this proceeding as one of four key planned results for the upcoming 12 months in its "Plans at a glance" to

> [i]mprove Canadians' trust in Canadian communications networks and e-commerce by exploring options to filter malicious Internet traffic as well as options for necessary policy safeguards.[6]

4. We respectfully submit that, to the extent the current proceeding is motivated by specific concerns or fact patterns, their disclosure on the record of this proceeding will better ensure that they are addressed.

5. We are, nonetheless, pleased to respond to this call, , which we underline is focused exclusively on immediate technical threats that frustrate use of the internet itself, and on developing the safeguards that will ensure these not be used to block content or online speech—for which more proportionate remedies exist, if required at all.

6. CIRA is a member-based not-for-profit organization best known for managing the .CA internet domain on behalf of all Canadians, developing and implementing policies that support Canada's internet community, and representing the .CA registry internationally. Our activities are focused on four key areas, each engaged in different aspects of the ecosystem that forms the context for this proceeding:

   - Our core mission is to ensure the safety and security of the .CA domain, including its domain name system ("**DNS**"), registry, and other related underlying technologies.
   - Our international registry services provide a platform relied on by top-level domain administrators around the world.
   - Our cybersecurity services include CIRA Anycast DNS, the secondary DNS service for which we operate networks and equipment across Canada and on five continents internationally; and CIRA DNS Firewall, through which network operators and businesses protect their networks at the DNS level.
   - Our community benefit activities to improve Canada's internet include Community Investment Program grants; support for internet exchange points; the CIRA Internet Performance Test; and CIRA Canadian Shield, a user-level version of our DNS Firewall service, to which the Notice refers.

7. Like many other internet bodies and stakeholders, it is CIRA's view that network-level blocking is a blunt and extreme remedy—rarely necessary, generally disproportionate, and antithetical to the policy of net neutrality that is the fundamental ethos of the internet and its legacy of permissionless innovation.

8. We therefore approach the topic of this proceeding not only with surprise, as described above, but with great caution. It is fundamental to this proceeding, and to CIRA's submissions, that even the strongest approach available to the Commission at law—a section 36 approval framework that would permit Telecommunications Service Providers ("**TSPs**") to elect to engage in network-level blocking—be focused on imminent technical theats to network integrity and, therefore, use of the internet.

9. A key outcome will, therefore, be the safeguards that ensure that such a framework not only is not allowed to be, but cannot from a technical standpoint, be used for content-blocking or -filtering. These include ensuring that blocks are ordered by certified independent parties, not TSPs, many of which are

---

[5] Indeed, the Yale Report (note 3 above, recommendation 45) specifically called for an amendment to insert, into the *Telecommunications Act,* a policy objective related to network security.

[6] Page 5.

vertically-integrated and have an incentive to provide for leakage between the compartments we say must remain watertight. These also include automated monitoring of such blocking in order to generate comparisons between what independents have designated for blocking, and what TSPs have actually blocked.

10. They include further measures, too, set out in the course of CIRA's detailed submissions below. Our intervention groups its responses to the Notice's questions by subject area, beginning with Section A **(Jurisdiction—Q7 and Q1**, paragraphs 14-4746) addressing the basis on which the Commission proposes to address the issue it has identified, and the limited scope which its governing statutes provide for it to do so. In CIRA's view, the *Telecommunications Act*[7] provides jurisdiction for a network-level blocking framework only on a non-mandatory basis, by way of clarifying under which conditions it will approve such activities as compatible with the common carrier role of TSPs. We outline why such a framework must centre transparency, non-discrimination, necessity, and proportionality as animating principles.

11. Sections B, C, D, and E then address the four[8] sets of necessary safeguards summarized at paragraph 15 of the Notice, with a particular focus on **Privacy (Q2**, Section B**,** paragraphs 48-61) and **Accountability** (**Q3- Q4**, Section C, paragraphs 62-79).

12. In respect of privacy safeguards, the Commission's long-standing practice is to impose a higher standard than that available under PIPEDA,[9] and it should do so here. In respect of accountability safeguards, we call for any section 36 approval framework to incorporate programmatic transparency, by requiring disclosure of blocking plans and regular transparency reporting; user-level transparency, by coordinating information standards by which TSPs could elect to incorporate botnet notifications into their notice-and-notice activities; and procedural transparency measures, by coordinating different disclosure standards. Further safeguards, addressed in Sections D (**Defaults—Q5**, paragraphs 80-83) and E (**Accuracy—Q6**, paragraphs 84-88), speak to safeguarding users' right to opt out, in the likely eventuality that many TSPs elect an opt-out approach; and to mandatory accuracy and verification features, including certified list provider responsiveness, user lookups and APIs, a right to root cause analysis, and building integrity into block log comparisons to identify improper TSP-originated blocks.

13. Finally, Section F (paragraphs 90-102) addresses **Technical Design**, on which the greatest number of questions is posed (**Q8, Q9, Q10**) but which, in CIRA's view, are better focussed on ecosystem interoperability, the right of end-users to choose their own intermediaries, and the Commission's responsibility to ensure they have the information to make informed choices, followed by concluding remarks (Section G, paragraphs **Error! Reference source not found.**-106).

A. <u>Jurisdiction</u> (Q7, Q1)

Q7. What regulatory mechanism is best suited to ensure implementation of a network-level blocking framework that effectively addresses botnet communications?

14. Although positioned seventh among the questions posed by the Notice, the threshold question of jurisdiction is fundamental to the scope of this proceeding, and so we address it here first.

---

7 S.C. 1993, c. 38.

8 Note 2, above.

9 *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5.

15. The Notice canvasses the use of sections 24 and 24.1, 42, 41, and 36 in relation to a network-level blocking framework. In response and for the reasons set out below, it is not open to the Commission to adopt a general scheme for mandatory network blocking under sections 24 and 24.1 of the *Telecommunications Act*, nor any kind of network blocking under sections 42 or 41.

16. But clarifying the conditions under which it would grant approval to a TSP seeking, under section 36 of the Act, to block in- or outbound traffic in order to remediate botnets, is open to the Commission. Doing so could help safeguard the policy of net neutrality that is a key priority for the Government of Canada;[10] CRTC;[11] Internet Society,[12] whose role we underline in sustaining the internet to which this proceeding pertains; and CIRA. That is because a section 36 approval framework would establish independent oversight, and principles and bases, on which TSPs may block traffic for "network security and integrity purposes"[13], including when such blocking or redirection is "for the purposes of network management" [14]—activities in which they likely already engage of their own accord anyway.

17. At the same time, CIRA is deeply concerned that any such voluntary framework be hijacked for purposes that in any manner stray from network integrity and security. The end-result of this proceeding, or of the Commission's activities in this area, must not be the development of a more accessible master switch that nudges common carriers towards a role as editors, filters, or sheriffs of the internet. It is therefore essential that any section 36 botnet-blocking approval framework centre the principles of transparency, non-discrimination, necessity, and proportionality, for the reasons set out below; and work carefully to avoid the possibility of regulatory capture or single points of failure, for the reasons then set out in the remainder of this intervention.

Sections 24 and 24.1

18. The Notice relates to the "harm caused to Canadians by botnets". Its goal in propounding a "network-level blocking" framework to prevent such harm[15] is to:

---

10 Innovation, Science and Economic Development Canada, *Terms of reference* (establishing a Broadcasting and Telecommunications Legislative Review), 2018 ("Net neutrality is a key Government priority given its importance for freedom of expression and the 'innovation without permission' ethos that underpins the success of the Internet…. Net neutrality principles must continue to be a core part of future legislation while giving the regulator the flexibility needed to consider new developments and adapt accordingly.").

11 CRTC, "Strengthening net neutrality in Canada", https://crtc.gc.ca/eng/internet/diff.htm ("Why does the CRTC support net neutrality? We believe that it is important that all Canadians have access to choice, innovation and free exchange of ideas. Internet providers should compete on the quality of their networks, by lowering their prices or increasing data allowances instead of treating certain content differently. In the past few years, we have issued many decisions in order to support net neutrality.").

12 Internet Society, "Policy Brief: Network Neutrality", 30 October 2015 ("Guiding Principles" delineating, among other matters, reasonable network management practices).

13 *Review of the Internet traffic management practices of Internet service providers,* Telecom Regulatory Policy CRTC 2009-657, 21 October 2009, paragraph 44 ("The Commission notes that Canadian ISPs have used certain ITMPs for the purposes of network security and integrity. Specifically, these ITMPs have been employed to protect users from network threats such as malicious software, spam, and distribution of illicit materials."). In CIRA's view, however, the approach to be taken to the "distribution of illicit materials" is different than that to be taken to activity that harms network integrity, for the reasons set out in this intervention.

14 S.C. 2010, c. 23 ("**CASL**"), subsection 7(2) (prohibition on altering transmission data "does not apply if the alteration is made by a telecommunications service provider for the purposes of network management").

15 Notice, paragraphs 8, 14, 17, 26, and 35 (harm reduction goal).

- address what is "by definition a CASL violation", including expanding on the Commission's interpretation of its discretion under CASL's section 9 prohibition "to aid, induce, procure or cause to be procured" illegitimate spam distribution, malicious network traffic redirection, or malware installation activities"[16]—noting that the Commission "does not have the authority and mandate to use the regulatory mechanisms in the "[Telecommunications] Act to address malicious activity facilitated by botnets"; and,
- "promote the [Telecommunications] Act's policy objectives", to which end the Notice underlines that "[m]alicious activity facilitated by botnets"—or, at least, the result of such activity—"is contrary to several of the Act's policy objectives", insofar as malicious activity disturbs the Canadian telecommunications system's development, accessibility, ability to meet user needs, and ability to protect privacy.[17]

19. In contrast to the enabling statutes of other communications regulators, including those of the U.S., Germany, and the U.K., the policy objectives of the *Telecommunications Act* do not include "the promotion of the security and reliability of telecommunications networks and … services". The Yale Report recommended that this objective be inserted into section 7 of the Act.[18] It has not yet been.

20. On the narrow issue of the Commission's view that "it has a number of powers under the Act that would allow it to establish either a mandatory or voluntary framework",[19] mandatory and voluntary frameworks should therefore be distinguished carefully. It is one thing to point to the very real harms that unchecked botnets wreak on the ability to use telecommunications services. It would be quite another to find that, even in the combined presence of *(a)* already-existing private-sector remediation services, including CIRA's, and *(b)* any voluntary network-level blocking framework that emerges from this proceeding, the harms remain so great that the continuing ability of Canada's telecommunications system to meet the Act's existing policy objectives depends on making mandatory blocking orders.

21. The improbability of such a finding is illustrated by the internet's continued functioning absent even the voluntary framework that may be established following this proceeding. Absent such a finding, the *Telecommunications Act* does not grant jurisdiction for the Commission to create a general framework ordering TSPs to block in- or outbound traffic under sections 24 or 24.1. The Commission may exercise the powers created by these sections of its own motion only with a view to implementing the policy objectives as they stand today. Absent a finding of necessity, which is improbable for the reasons set out above, mandatory blocking is not necessary to achieving those policy objectives, and is not open to the CRTC to order.

22. CIRA acknowledges that specific facts could arise in which an intervener or the Commission believed an urgent mandatory blocking order necessary and proportionate for remediating network harm that was otherwise materially impairing achievement of Canada's telecommunications policy objectives. If so then, it is submitted, the Commission would be required to convene an expedited proceeding under the *Telecommunications Act* applying its requirements, including the transparency it properly mandates, to the facts at hand.[20] Similarly, should the Commission be of the view that past facts demand the *ex ante*

---

16 Notice, paragraphs 5-8.

17 Notice, paragraphs 4 and 14 (goal to further the policy objectives of the *Telecommunications Act,* note 7 above).

18 Yale Report, note 3 above, recommendation 45 and accompanying text (comparing regulatory responsibility for communications security in Canada to that of other jurisdictions).

19 Notice, paragraph 33. (Paragraphs 33-35 elaborate on Q7.)

20 *Practices and procedures for dispute resolution,* Broadcasting and Telecom Information Bulletin CRTC 2019-184, 29 May 2019, paragraphs 34-45.

establishment of a framework under which such an order could be made, it has the ability to put those facts on the record.

Section 42

23. In relation to section 42 of the *Telecommunications Act,* which the Notice surmises that the Commission "could also consider … to extend this framework to other persons [than Telecommunications Service Providers] who have control over telecommunications facilities", we respectfully remind the Commission that this section, helpfully captioned "Works ordered by Commission" under the general heading of "Construction and Expropriation Powers", relates to the Commission's power to "require or permit

- any telecommunications facilities to be provided, constructed, installed, altered, moved, operated, used, repaired or maintained or
- any property to be acquired or any system or method to be adopted[.]"

24. To read the latter words "any system or method to be adopted" in a manner divorced from the remainder of the section would be wholly inconsistent with the requirement to read these words and derive their meaning from "their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act", particularly as "a component of a larger statutory scheme [in which] the surroundings that colour the words and the scheme of the Act are more expansive."[21]

25. On the contrary. It is clear from the context, scheme of the Act, and surroundings that colour the words and scheme, that section 42 as a whole relates to physical telecommunications "facilities" (each a "facility, apparatus, or other thing") and the power to "order that work be done on [them] and to order expropriation of property for that purpose".[22] Construction and expropriation powers over physical works relate to activities at an utterly different layer, or level, than network-level blocking. It is not open to the Commission to mobilize the former powers for the latter purpose.

Section 41

26. Section 41 of the *Telecommunications Act* was introduced in 1993 so that the CRTC could make orders that

> prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications to the extent that the Commission considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression.

27. Under this limited power to regulate unsolicited telephone calls, the Commission adopted a policy prohibiting the use of automated dialing-announcing devices, known as "robocalling", for commercial solicitation. The Commission adopted this policy after having considered, and concluded, that such a prohibition was narrowly-tailored enough to constitute such reasonable limit on the guarantee of freedom

---

21 *Bell ExpressVu LP v. R.*, 2002 SCC 42, paragraphs 26-27, citing E. Driedger, Construction of Statutes (2nd ed., 1983), page 87), further cited in *Reference re Broadcasting Regulatory Policy 2010-167 and Broadcasting Order CRTC 2010-168*, 2012 SCC 68, paragraphs 11-12.

22 *Telecommunications Act,* note 7 above, section 42 and subsection 1(1) (definition of "telecommunications facility"); *Calgary (City) v. Bell Canada Inc.*, 2020 ABCA 211, paragraph 49 (characterizing the grant of authority made by section 42).

of expression as could be demonstrably justified in a free and democratic society, in respect of a practice that "clearly cause[s]" undue inconvenience, nuisance, and invasion of privacy to subscribers.[23]

28. In 2010, CASL was passed, providing for section 41 to be amended by renumbering it as subsection 41(1) and adding a subsection 41(2) to specify that this power to prohibit or regulate facilities use for the provision of unsolicited telecommunications cannot be used to prohibit or regulate the use of telecommunications facilities for carrying a "commercial electronic message"—for which we have, instead, CASL.

29. Subsection 41(2) was not worded, however, so as to specify explicitly whether the regulatory power that is unavailable in respect of "commercial electronic messages" might, in fact, be available in respect of another activity to which "Canada's anti-spam law" relates, *i.e.* installing computer programs uninvited. Instead, it is silent on the matter. The Notice invites comment on whether subsection 41(2)'s silence might, perhaps, be read as authorizing the CRTC's use of subsection 41(1) to regulate, not just unsolicited nuisance telephone calls but now, also, the unsolicited installation of computer programs, as botnets infecting a device with a Trojan or drive-by download might do over the Internet.

30. In CIRA's view, and with respect, such a reading appears both strained and redundant. When adopted nearly 30 years ago, what is now subsection 41(1) was by all accounts intended only to relate to telephone calling. It is difficult to support the notion that, in then limiting its scope explicitly in 2010, the wording CASL selected incorporated studious silence about computer program installation, not because its drafters did not consider that anyone could read it in such a way, but because they in fact intended to enable regulation of Internet traffic related to such unauthorized installation. Such a significant but unannounced change is, we submit, not consistent with the context of which statutory interpretation must be mindful. The better and more reasonable interpretation is that subsection 41(2)'s exclusionary language focussed on unsolicited nuisance calls and their electronic equivalent, spam, simply because that was the topic at hand. The provision's subject matter is nuisance communications, not surreptitious installations, as demonstrated amply by the section's reference to "undue inconvenience and nuisance".

31. To extend subsection 41(1) beyond nuisance telephone calls to cover network-level internet blocking would, in any case, also be redundant. The unlikely argument that subsection 41(1) could underwrite a mandatory network-level blocking scheme butts up against the same concerns raised earlier with respect to sections 24 and 24.1, only with a higher hurdle. The proponent would have to show that such a limitation—as opposed to a voluntary scheme in tandem with already-existing tools—is not "undue" and is minimal and proportionate in a manner that "giv[es] due regard to freedom of expression". An argument that subsection 41(1) could underwrite a voluntary, rather than mandatory, network-level blocking scheme would, for its part, fail to relieve the need for the Commission to grant parallel approval under section 36,[24] and fail to introduce a lower standard for obtaining it. There appears, therefore, little purpose for the Commission to consider the role that section 41 plays in any scenario, regardless of how well- or ill-founded.

---

23 *Use of telephone company facilities for the provision of unsolicited telecommunications,* Telecom Decision CRTC 94-10, 13 June 1994, updating *Use of Automatic Dialing-Announcing Devices*, Telecom Decision CRTC 85-2, 4 February 1985. A further enactment to permit the Commission to administer databases for the purpose of its power under section 41, and to apply related administrative monetary penalties, was made in S.C. 2005, c. 50, adding sections 41.1 through 41.7.

24 That "[i]f it is reasonably possible so to construe the provisions as to give effect to both [provisions], that must be done" is a trite principle of statutory interpretation. 36 Hals., 3rd ed., p. 365, cited in *Daniels v. White*, [1968] SCR 517 (Judson J., maj.), page 526

Section 36

32. Telecommunications service providers require prior Commission approval before they may lawfully block traffic.[25] For instance:

> the Act prohibits the blocking by Canadian carriers of access by end-users to specific websites on the Internet without prior Commission approval, whether or not such blocking was the result of an Internet traffic management practice. Such blocking would only be approved where it would further the telecommunications policy objectives set out in section 7 of the Act. Accordingly, compliance with other legal or juridical requirements—whether municipal, provincial, or foreign—would not, in and of itself, justify the blocking of specific websites by Canadian carriers, in the absence of Commission approval under the Act.[26]

33. This sets up a scheme that is particular to telecommunications common carriers. A TSP may wish to block traffic for purposes, like compliance with Quebec gambling regulation, or to enhance network security and integrity, that lie outside the policy objectives around which the *Telecommunications Act* is built. Yet the TSP must have the Commission's permission to do so; and the Commission may only grant that permission as against the Act's policy objectives.[27]

34. In a world in which virtually all meaning is sooner or later conveyed by means of transmission facilities, this scheme inserts the CRTC into topics whose putative substance does not relate to its mandate, from copyright infringement to gambling licensing to cybersecurity—but whose proposed remedy falls squarely into it. That underlines the important role that TSPs play as common carriers, to which net neutrality is closely related, and which Parliament made it the CRTC's task to interpret and safeguard.

35. CIRA agrees that, for the purposes of clarifying that role, it would be helpful for the Commission to delineate carefully the principles and bases on which TSPs can lawfully block traffic for network security and integrity purposes, such as botnet-related traffic. This should include delineation of when the blocking or redirection of telecommunications traffic is solely "by a telecommunications service provider for the purposes of network management",[28] which today likely takes place without such oversight:

> To protect the [Canadian TSP]'s infrastructure, its customers, and the Canadian telecommunications critical infrastructure, CTSPs need to have the capacity to filter or to drop traffic that is causing significant damage to themselves or others.
>
> Note: this section concerns traffic that the CTSP deems to be harmful to its network, or harmful to other providers' networks and is intended for the mitigation and remediation of such traffic. It

---

25 *Telecommunications Act,* note 7 above, section 36. It should be noted that this section refers to whether the carrier "controls the content or influence[s] the meaning or purpose of telecommunications carried by it for the public." In our view, the equal applicability of this section to traffic blocking measures that relate to content, and to network security and integrity, is well-settled and, in any case, difficult to distinguish. Any blocking of telecommunications traffic would, for instance, certainly influence its purpose.

26 *Public Interest Advocacy Centre – Application for relief regarding section 12 of the Quebec Budget Act,* Telecom Decision CRTC 2016-479, 9 December 2016, paragraphs 7 (setting out a "preliminary view"; emphasis added) and 18-21 (confirming this preliminary view on the basis of "the legislative history of section 36, Canadian principles of statutory interpretation, and relevant jurisprudence").

27 *Telecommunications Act,* note 7 above, paragraph 47(a).

28 CASL, note 14 above, subsection 7(2) (describing the circumstances in which subsection 7(1)'s general prohibition on alteration of transmission data "in an electronic message" does not apply).

> does not oblige CTSPs to block content that a third party finds objectionable, but merely states the controls that should be in place, so the CTSP can act when warranted.[29]

Absent a principled section 36 approval framework, TSPs are left to decide unilaterally which traffic is harmful, whether and under what conditions a user opt-in or -out may occur, which privacy safeguards to enact, and other determinations that the Notice establishes require independent user safeguards.

36. The Commission's approach to conditions of approval for technical network management practices, a parallel activity, focuses on whether the service provider is employing them in a way that is *(a)* transparent with respect to the practice being undertaken, the need for it, its purpose and effect, and whether discrimination or preference results; and if such discrimination or preference does result, then whether it *(b)* is limited to the purpose and effect in question, *(c)* discriminates or prefers as little as reasonably possible, *(d)* can be demonstrated to harm other persons as little as reasonably possible, and *(e)* comes with an explanation as to why less invasive practices, that do not involve plunging one's metaphoric hand into the traffic stream, wouldn't reasonably address the need and, effectively, achieve the same purpose.[30]

37. In CIRA's view this approach based on *transparency*, *non-discrimination*, *necessity*, and *proportionality*, developed to gird the application of statutory undue preference rules to ISPs' traffic management practices, will assist equally with considering:

- under which limited conditions, and
- the basis for the necessary related safeguards described in the Notice,

to approve a TSP's blocking of traffic for the purpose of remediating harms to network security or integrity.

38. CIRA's view stems from the proximity of an approach based on these four principles to what we understand to be international best practice—which does not always distinguish between traffic management and traffic blocking. The equivalent provisions of the EU Open Internet Regulation establishing net neutrality rules across Europe, for instance, state in part:

> Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.
>
> The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.
>
> Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down,

---

29 Canadian Security Telecommunications Advisory Committee (CSTAC), *Security Best Practice for CTSPs* (version 1.1), 20 January 2020, section 5.3 (entitled "Remediation and Mitigation of Malicious or Inappropriate Traffic"), emphasis added.

30 TRP 2009-657, note 13 above, paragraph 43.

> alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary…[31]

Technical guidance on these provisions goes on to caution that

> whether or not a security measure is justified … depends on the circumstances, the type of networks, services, etc. Security is a fast moving field and cyber-attacks are changing constantly. What may have been an effective measure at one point in time, in the middle of a large-scale attack for instance, may be considered as unnecessary and disproportionate later on.[32]

39. CIRA therefore urges the Commission to adopt as foundational, to its section 36 review of the framework under which TSP botnet-related traffic blocking measures would be permitted, the principles of transparency, non-discrimination, necessity, and proportionality.[33]

Q1. As a Canadian Internet user, how would you benefit from having your TSP block malicious botnet communications? What concerns do you have?

40. CIRA appreciates the Commission's focus on internet users in this proceeding. In promoting a trusted internet for Canadians and in maintaining accountability to our ultimate stakeholders, we hold regular informal and formal meetings with Canadian internet users and conduct annual surveys and studies on what they identify as key issues facing the internet.

41. What we have learned is that Canadians depend on the internet, have strong views about the internet, and have a sophisticated understanding of internet policy and its contradictions. As we suggested in the foreword to our first post-COVID report in 2020, *Canadians Deserve a Better Internet,*

> Canadians now feel that it's time for the government and global internet governance stakeholders to act and provide new safeguards for internet users. The point of any policy or regulation should be to provide an equalizing force – to ensure individual rights aren't eclipsed by entrenched interests, that modern convenience doesn't come with a price tag of forfeiting privacy, and that facts aren't clouded out by fiction. Working together, we can strike the right

---

31 Regulation (EU) 2015/2120, 25 November 2015, article 3(3).

32 *Guidelines on assessing security measures in the context of Article 3(3) of the Open Internet regulation*, European Network and Information Security Agency (ENISA), December 2018, page 4.

33 It has elsewhere been put that similar principles should also apply to traffic-blocking frameworks more broadly. The six *Manila Principles on Intermediary Liability,* which relate to content-oriented traffic blocking, hold that

1. "Intermediaries should be shielded from liability for third-party content";
2. "[c]ontent must not be required to be restricted without an order by a judicial authority";
3. "[r]equests for restrictions of content must be clear, be unambiguous, and follow due process";
4. "[l]aws and content restriction orders and practices must comply with the tests of necessity and proportionality";
5. "[l]aw and content restriction policies and practices must respect due process"; and
6. "[t]ransparency and accountability must be built into laws and content restriction policies and practices."

While focused heavily on content restrictions, certain guidance provided in respect of the fourth (necessity and proportionality and sixth (transparency and accountability) principles—limiting scope and duration through periodic framework review; transparency reporting to summarize actions taken; independent, transparent, and impartial oversight mechanisms—are germane in respect of network-integrity-oriented blocking, as discussed below.

> balance that provides the regulation Canadians need for the internet to be a part of this country's future health and prosperity.[34]

42. We learned that Canadians care deeply about privacy, net neutrality, and provider choice, and insist that the trusted internet they deserve be reconciled with these. The vast majority were not willing to share their personal data in exchange for better services. More than 80 percent believed it important that government data, including their personal information, be stored and transmitted in Canada only—and about the same number supported giving the Office of the Privacy Commissioner stronger powers. About two thirds supported the principle of net neutrality. About 60 percent not only wanted more choice in service providers, but supported a requirement to mandate wholesale mobile supply to do it.

43. Canadian Internet users, we respectfully submit, do not see privacy and security, or net neutrality and security, or provider choice and security, as trade-offs to be opposed to one another. They see these as important values that it is our job, as telecommunications and internet professionals, to reconcile.

44. Others are engaged in a similar job. When staff in the U.S. Departments of Commerce and Homeland Security were tasked, in 2017, to react to an Executive Order calling for "resilience against botnets and other automated, distributed threats", the resulting *Road Map Toward Resilience Against Botnets* defined 85 tasks within five "lines of effort". One of these lines of effort, "Internet Infrastructure", related in part to ISPs. The following describes one of its four workstreams:

> Large network providers currently share network management techniques and defensive tactics that are effective against particular threats. Law enforcement depends upon information from the private sector to initiate investigations. This series of tasks focuses on extending information sharing to smaller ISPs and foreign network providers, and ensuring that law enforcement is alerted at the earliest possible stage, while respecting privacy guidelines and regulations.[35]

45. Operational data generated in the course of delivering CIRA Canadian Shield and CIRA DNS Firewall indicate that work-at-home scenarios have created new cybersecurity threat vectors. These deepen the need, among Canadian Internet users, for better-adapted cybersecurity training,[36] but also increase the cybersecurity risk profile and burden shouldered by consumer-focused ISPs.

46. CIRA knows well that many of these ISPs, with whom we work, already faced relentless and endless barrages of malicious traffic pre-pandemic, which have worsened as the risk profile and burden have increased. And we understand that telecommunications providers cannot lawfully block malicious traffic without Commission concurrence.

47. However, we underline that such concurrence must be based on a framework that gives full effect to the policy objectives of the *Telecommunications Act.* Any section 36 approval framework for network integrity measures must not materially weaken net neutrality, or Canadians' privacy, or service provider choice or market permeability. It must not introduce a slippery slope or convenient kill switch with the ability to alter the careful balance struck by Parliament and by the CRTC in respect of content-oriented measures. Commission concurrence must be extended only in respect of lawful blocking of malicious network traffic whose framework is transparent, non-discriminatory, necessary and proportionate. It is on that

---

34 Ottawa, 2020. Online: <https://www.cira.ca/resources/state-internet/report/canadians-deserve-a-better-internet-2020>.

35 U.S. Departments of Commerce and of Homeland Security (Washington, DC, November 2018), page 18.

36 *CIRA Cybersecurity Report 2020* (under "Cybersecurity Awareness Training for Organizations"). See also "Cybersecurity practices for remote workers", an online free cybersecurity course that CIRA has made available as part of its work to help the Canadian internet respond to the COVID-19 pandemic.

basis that we recognize the value of establishing in and through this proceeding, and any follow-ups from it, a careful framework that exercises independent oversight to ensure that the values Canadian internet users espouse—like privacy, net neutrality, and provider choice—are preserved as we build Canada's internet forward.

B. Privacy (Q2)

Q2. What framework conditions are required to safeguard Internet service subscribers' privacy during traffic monitoring and blocking program reporting?

48. Whereas promoting the security of Canadian telecommunications networks is not one of the *Telecommunications Act*'s policy objectives, "contribut[ing] to the privacy of persons" is.[37]

49. The Commission's telephone consumer confidentiality safeguards[38] prohibit TSPs from disclosing customer information other than name, address, and listed phone number to any person other than the customer except "pursuant to a legal power"[39] or to defined exceptions.[40] The Commission has described these safeguards as, in certain respects, establishing "a higher standard of privacy protection than that which would be available under the PIPED Act"—which is

> even more relevant today than when the [customer confidentiality safeguard] provisions were first implemented, due to the advent of new technologies and the emergence of electronic commerce, which allow information to be more easily processed, rearranged and exchanged. The

---

37 Note 7 above, paragraph 7(i).

38 *Review of the general regulations of the federally regulated terrestrial telecommunications common carriers,* Telecom Decision CRTC 86-7, 26 March 1986, as updated (note 40, below).

39 *Provision of subscribers' telecommunications service provider identification information to law enforcement agencies*, Order CRTC 2001-279, 30 March 2001; *Provision of subscribers' telecommunications service provider identification to law enforcement agencies*, Telecom Decision CRTC 2002-21, 12 April 2002.

40 Last updated in *Regulatory measures associated with confidentiality provisions and privacy services*, Telecom Regulatory Policy CRTC 2009-723, paragraphs 6-21 and Appendix, expanding the list of exceptions to the following six (new addition added):

- "a person who, in the reasonable judgment of the company, is seeking the information as an agent of the customer;
- another telephone company, provided the information is required for the efficient and cost-effective provision of telephone service and disclosure is made on a confidential basis with the information to be used only for that purpose;
- a company involved in supplying the customer with telephone or telephone directory related services, provided the information is required for that purpose and disclosure is made on a confidential basis with the information to be used only for that purpose;
- an agent retained by the company in the collection of the customer's account, provided the information is required for and is to be used only for that purpose;
- a public authority or agent of a public authority, for emergency public alerting purposes, if a public authority has determined that there is an imminent or unfolding danger that threatens the life, health or security of an individual and that the danger could be avoided or minimized by disclosure of information; or
- an affiliate involved in supplying the customer with telecommunications and/or broadcasting services, provided the information is required for that purpose and disclosure is made on a confidential basis with the information to be used only for that purpose."

> Commission also considers that, as its own experience in dealing with privacy issues has demonstrated, technical expertise and specific telecommunications industry knowledge is often required to address privacy-related issues in the telecommunications industry.[41]

50. Unlike the U.S. Federal Communications Commission,[42] and notwithstanding a commitment to "shift[ing] the focus of its current regulatory frameworks from wireline voice services to broadband Internet access services",[43] the CRTC has not yet sought to adapt its telephone consumer confidentiality safeguards to the broadband environment. However, in fulfilling its obligation to exercise its powers to contribute to the privacy of persons, the CRTC has intervened in a more targeted way with respect to traffic management "technologies [that] have the capacity to collect and use personal information … [which] can be derived from the flow of network traffic, without the knowledge or consent of the consumer". In doing, the Commission again considered that "it would be appropriate to impose a higher standard than that available under PIPEDA in order to provide a higher degree of privacy protection for customers of telecommunications services":

> The Commission therefore directs all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information…. [and] to include, in their service contracts or other arrangements with secondary ISPs, the requirement that the latter not use for other purposes personal information collected for the purposes of traffic management and not disclose such information.[44]

51. The Notice seeks comment on "conditions that can protect consumer privacy", like prohibiting the processing of content or metadata that does not contribute to blocking botnet traffic; limiting monitoring and collection to destination and frequency—which is deeply personal information about what a person is thinking about when and how often; and restricting disclosure to "parties participating in the blocking program".

52. In response, we respectfully note that the Commission's statutory obligations, and the manner in which it has applied them in the past, create the following legitimate expectation. Absent very good reasons to the contrary, any filtering options for malicious internet traffic that the Commission now wishes to explore by way of a section 36 exemption, must be accompanied by privacy safeguards that "impose a higher standard than that available under PIPEDA", by applying the "technical expertise and specific telecommunications industry knowledge" the Commission brings to bear, to the extent "required to address privacy-related issues in the telecommunications industry".

53. Such an expectation would be consistent with Canadian privacy law's approach to TSPs' role as agents "to whom users must entrust vast amounts of their sensitive personal information in order to gain access to mobile, internet, telephone and television communications in Canada"[45]—in other words, with the

---

41 *Forbearance from the regulation of retail local exchange services,* Telecom Decision CRTC 2006-15, 6 April 2006 (as modified on other grounds by Order-in-Council PC 2007-532, 4 April 2007), paragraph 366.

42 *In the matter of protecting the privacy of customers of broadband and other telecommunications services*, FCC 16-148, 2 November 2016, as nullified followed issuance of Public Law 115-22 pursuant to the Congressional Review Act (U.S.).

43 *Modern telecommunications services—The path forward for Canada's digital economy*, Telecom Regulatory Policy CRTC 2016-496, 21 December 2016.

44 TRP 2009-657, note 13 above, paragraphs 102-104.

45 *Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program,* PIPEDA Report of Findings 2015-001 (OPC), 7 April 2015.

role of telecommunications providers as obligatory passage points for participating in a digital Canadian society. The same expectation would be consistent with Canadian telecommunications law's express delegation, to the Commission, of the earlier-discussed responsibility to safeguard common carriage.

54. But to prohibit personal information processing in traffic that does not contribute to the purpose at hand, or to limit generally what is monitored and collected to no more than what is required for that purpose, or to restrict the disclosure of such collection to a circle of trust, does not "impose a higher standard than that available under PIPEDA". Without further elaboration, these guidelines mooted at paragraph 22 of the Notice could even induce TSPs to meet a lower standard, such as the lower standard currently elaborated in CSTAC's draft Security Best Practices.[46]

55. The Notice goes on, under the heading of Q2, to seek comment on highly specific implementation details like "the appropriate metrics to use to ensure the framework is functioning as intended. Examples include the timestamps and volumes of blocking events and the false-positive rate."

56. It is, with respect, inappropriate at this stage of this proceeding; inappropriate at this stage of the Commission's new and different interest in establishing security guidelines for Canadian TSPs; and inconsistent with basic cybersecurity guidance,[47] to enter into this level of detail before establishing general principles and governance frameworks for achieving them. Take, instead, the success metrics on which the Notice seeks guidance under the heading of "subscribers' privacy" as shorthand for the need for public transparency reporting, by any blocking ISPs, at established intervals to specified metrics that help users confirm that the purpose underwriting controlled incursions into their privacy is, indeed, one that is worthy because it is functioning as intended.

57. That, however, begins to stray from the privacy purpose identified in Q2 as a key "safeguard" area to be met if a network integrity blocking framework is to pass muster on a section 36 dispensation. Any such framework should establish privacy standards and principles to be met, so that TSP-specific blocking programs (if any) can be reviewed against these and found either acceptable or wanting. Such a framework should demonstrate transparency, non-discrimination, necessity, and proportionality but, in doing so, require compliance with applicable private-sector privacy laws and with relevant industry standards.

58. The basic privacy principle retained in the ITMP framework should be retained here. Information collected for the purposes of botnet remediation should not be used or disclosed for any other purpose, nor retained except to the extent strictly required for this sole purpose.

---

46 *Security Best Practice for CTSPs,* note 29 above, at section 6.3 (entitled "Privacy"), which correctly notes that privacy rights constitute "legal requirements [that] take full precedence over the guidelines listed in these best practices", and then goes on to state that "[t]he CTSP serving a customer must be able to identify the user who is the source or target of malicious activities, but this information should not be shared with other entities unless disclosure is done in accordance with the requirements of the provider's Privacy Policies *(sic)* and Terms of Service" (emphasis added). Legal requirements that take precedence over this guidance would further specify in what ways the CTSP would have to be able to identify the user; and would further narrow the circumstances, if any, under which such information should be shared with other entities.

47 See, *e.g.,* U.S. National Institute for Standards and Technologies, *Framework for Improving Critical Infrastructure Cybersecurity* (version 1.1), 16 April 2018 ("**NIST Cybersecurity Framework**") describing, at page 13, "life cycle phases of plan, design, build/buy, deploy, operate, and decommission. The plan phase begins the cycle of any system and lays the groundwork for everything that follows. Overarching cybersecurity considerations should be declared and described as clearly as possible."

59. Similarly, we note that the Best Practices maintained by the FCC's Communications Security, Reliability, and Interoperability Council ("**CSRIC**", which issued its own botnet guidelines nine years ago[48]) include the following:

> Service Providers should pursue a multi-prong strategy in designing technical measures for identification, notification, or other response to compromised end-user devices ("technical measures"), to protect the privacy of customers' information, including but not limited to the following:
>
> a) ISPs should design technical measures to minimize the collection of customer information;
>
> b) In the event that customer information is determined to not be needed for the purpose of responding to [these] security issues,[49] the information should promptly be discarded;
>
> c) Any access to customer information collected as a result of technical measures should at all times be limited to those persons reasonably necessary to implement the botnet-response security program of the ISP, and such individuals' access should only be permitted as needed to implement the security program;
>
> d) In the event that temporary retention of customer information is necessary to identify the source of a malware infection, to demonstrate to the user that malicious packets are originating from their broadband connection, or for other purposes directly related to the botnet-response security program, such information should not be retained longer than reasonably necessary to implement the security program (except to the extent that law enforcement investigating or prosecuting a security situation, using appropriate procedures, has requested that the information be retained); and
>
> e) the ISP's privacy compliance officer, or another person not involved in the execution of the security program, should verify compliance by the security program with appropriate privacy practices.[50]

60. This best practice addresses the principle of necessity by minimizing collection to, limiting access based on, and discarding information not required for, the purpose it was collected. It addresses the principle of non-discrimination by requiring regular audits that would verify appropriate and fair compliance, rather than assuming them.

61. It does not address the need for transparency, by ensuring that privacy safeguards such as hold periods are made public, as addressed below. It does not address explicitly the proportionality best practice of minimizing personal information processing by pseudonymizing or anonymizing data. Any section 36 approval framework to be developed as the eventual result of this proceeding should do so—alongside, to the extent possible, any general update of the telephone consumer confidentiality safeguards that the Commission may undertake.[51]

---

48 *CSRIC III Report on U.S. Anti-Bot Code of Conduct for Internet Service Providers,* FCC, 22 March 2012; *CSRIC III Report on U.S. Anti-Bot Code of Conduct for Internet Service Providers Barrier and Metric Considerations*, FCC, 14 March 2013.

49 As distinguished, for instance, from the prospect that the data may generally be useful for addressing unspecified or unidentified future security issues, which is not an acceptable such purpose.

50 *Communications Security, Reliability and Interoperability Council – Best Practices Database,* U.S. Federal Communications Commission, last updated 4 March 2021, Item 12-8-8923 (emphasis added).

51 CIRA notes, in this regard, interventions in the proceeding initiated by *Application regarding "COVID Alert" app, "ABTraceTogether" app and related matters,* Public Interest Advocacy Centre Part 1 application, CRTC File 8665-

C. Accountability (Q3, Q4)

Q3. What are the necessary disclosure requirements for carriers and TSPs to ensure Internet subscribers have sufficient information to make informed decisions about participating in a blocking program?

62. The Notice's discussion of this question is focused on substantive matters. It contemplates that there is a balance to be struck between "provid[ing] transparency about blocking programs", and putting "limits on what information is made available, since malicious actors could use any public information to circumvent the blocking measures."[52]

63. At the outset, it is important to underline that such a calculus is not a discretionary one to be adopted by the TSP, or Commission, shorn from surrounding obligations. Blocking for network integrity purposes and related monitoring involves processing personal information. Transparency includes disclosure of the reasons for that processing, whether related to inbound traffic blocking or outbound "walled gardening",[53] that privacy law demands be disclosed to the data subject. Especially in the context of the deliberative development of a principled approval framework, it is not enough to wave at PIPEDA's exception in respect of the processing being "reasonable for purposes related to investigating … a contravention of the laws of Canada or a province".[54] It must actually be reasonably demonstrated that such disclosure would likely prevent remediation. Doing so would have to overcome the prevailing current view that "security through obscurity" is not only a limited approach to security at best, but may actually weaken it.

64. At the substantive level, and based on this apprehension of transparency as the default any derogation from which must be justified, it is helpful to distinguish programmatic from user-level transparency.

Programmatic Transparency

65. In respect of programmatic transparency, we submit that both planning and performance disclosures are required:

- Planning disclosure involves the publication to users and prospective users of the approved, TSP-specific network integrity program that complies with any section 36 approval framework developed by the Commission, absent which such blocking would not be lawful. The information to provided should address not only inbound and walled-garden practices in respect of inbound and outbound network-level blocking, if any. It should also—if nothing else, as a matter of privacy law—make required disclosures in relation to personal information processing, such as the extent of collection and duration of retention.
- Performance disclosure involves transparency reporting to users and prospective users, at specified periodic intervals, of performance metrics of the type suggested by the Notice in relation to privacy,

---

P8-202005769, 9 September 2020, to the effect that the Commission ought to develop general guidelines and reporting standards in respect of TSP disclosure of broadband customer information.

[52] Notice, paragraphs 24-25.

[53] M3AAWG best common practices for the use of a walled garden: criteria for exit, entry, remediation and subscriber education when using a walled gawrden to remediate virus and bot-infections in subscriber devices (version 2.0), Messaging, Malware and Mobile Anti-Abuse Working Group, March 2015; Recommendations for the remediation of bots in ISP networks, RFC 6561 (IETF), March 2012, section 5.4.

[54] PIPEDA, note 9 above, paragraphs 7(1)(b), 7(2)(a), and 7(3)(c.1) and (d.1).

and to be specified once broad principles have been established and the details of a section 36 approval framework broached.

For efficiency, CIRA suggests that these be combined with the Commission's existing requirements related to Internet Traffic Management Practices disclosures.

66. This approach to programmatic transparency comports more generally with the sixth of the six Manila Principles on Intermediary Liability ("[t]ransparency and accountability must be built into laws and content restriction policies and practices"), which focus on content-oriented blocking but, we have argued, include approaches to accountability that are directly applicable to the current context. The following guidance is particularly germane:

> c) Intermediaries should publish their [blocking] policies online, in clear language and accessible formats, and keep them updated as they evolve, and notify users of changes when applicable….
>
> e) Intermediaries should publish transparency reports that provide specific information about all … restrictions taken by the intermediary, including actions taken on government requests, court orders, private complainant requests, and enforcement of … policies.[55]

67. Any section 36 approval framework for network-integrity-oriented blocking must publish both its corporate policies before the fact, and account for how they have been applied afterwards.

User-Level Transparency

68. In respect of user-level transparency, the Commission and this proceeding could play a useful role in setting information standards so as to better meet best practices like that promulgated by the EU's regional information security agency, ENISA, which states that

> [n]otifying end-users about remotely identified infections through their Internet Service Providers is a useful and effective approach (although ISPs should be given appropriate incentives for bearing the costs of this activity),[56]

and of FCC CSRIC, which adds that "Service Providers should ensure that botnet notifications to subscribers convey critical service information rather than convey advertising of new services or other offers".[57]

69. Consider, to that end, that *(a)* a variety of efforts exist to automatically observe compromised IP addresses and bring them to the attention of the organization to which they are registered, usually in a standard format; and *(b)* virtually all TSPs have now established notice-and-notice systems to automatically forward, to users leasing a particular Internet Protocol address at a particular time, notices from trusted sources that correctly implement an agreed markup format.

70. A helpful outcome from this proceeding could be coordination work to:

---

55 Manila Principles, note 32 above, page 5.

56 European Network and Information Security Agency (ENISA), *Botnets: Detection, Measurement, Disinfection & Defence* (Athens, 2011), pages 6 and 127-128.

57 FCC CSRIC Best Practices, note 50 above, Item 12-8-8918. In Canada, CASL guidance on segregating commercial electronic messages from messages consisting solely of information about an ongoing service may make such guidance redundant in any case.

- standardize a mark-up format in which botnet observatories could choose to format, and ISPs could choose to forward, notices to end-users in respect of observed infection; and
- set out best principles for a landing page to which such users could be directed.

With regard to the latter, it is important to acknowledge that the success or failure of botnet remediation frameworks to gain user credibility will relate substantially to the ability to connect it with broader efforts, since a section 36 approval framework, and indeed the role of the TSPs to which it applies, is a partial element at best.

71. The Internet Society's Online Trust Alliance guidance has long emphasized that whereas "[h]istorically, typical industry responses" to botnets relied "heavily on Internet Service Providers (ISPs) … recently remediation efforts have evolved to include other stakeholders and intermediaries", including security vendors, operating system providers, and Internet web sites and hosts.[58] Notification is a key vector in the prevention-detection-notification-remediation-recovery lifecycle mapped out in that best-current-practice guidance. Indeed, it is the only one which ISPs—rivalled, perhaps, by the most pervasive Web platforms, like Facebook or Netflix—may uniquely be able to play.

Procedural Transparency

72. Historically, tariffs and telephone books were the preferred medium of communication by which carriers made disclosures to customers.

73. The days of tariffs and telephone books have passed. However, both the Commission and the Commission for Complaints for Telecom-television Services ("**CCTS**") have from time to time set out guidelines in respect of actions by post-phone-book TSPs to inform their customers and potential customers of key consumer terms, whether posted prominently to a TSP Web site at a location no more than two or one links deep;[59] written and communicated in a way that is clear, accessible, and easy for customers to read and understand;[60] or otherwise. Similarly, a growing body of guidance is emerging in relation to so-called "layered" and "just-in-time" privacy notices as a key component of full and informed consent.[61]

74. The Commission and CCTS now appear to be increasingly in the position of assessing and evaluate all over again whether disclosure methods have been sufficiently specified, or sufficiently met, in a way that ensures transparency and implies the recipient's consent. CIRA suggests that the Commission consider whether, rather than continuing in a piecemeal manner, it ought to address the matter holistically in a follow-up proceeding.

Q4. Which parties are best suited to decide what is blocked?

75. The Commission's preliminary response to this question is that

---

58 Online Trust Alliance, *Botnet Remediation Overview & Practices* (Reston, VA: 1 October 2013), page 3.

59 *Call for comments – The Canadian Radio-television and Telecommunications Commission Accessibility Reporting Regulations,* Telecom and Broadcasting Notice of Consultation CRTC 2021-69, 18 February 2021, paragraph 47 ("Plans and reports must also be conspicuous in order to be readily discoverable. In this regard, they are to be published on a regulated entity's main digital platform (e.g. website or mobile application), either directly on the home page or no more than one click away from the home page.").

60 *The Internet code,* Appendix to Telecom Regulatory Policy CRTC 2019-269, 31 July 2019, Appendix A.1.ii.

61 *Guidelines for obtaining meaningful consent,* Office of the Privacy Commissioner (Canada), May 2018 ("Determining the appropriate form of consent").

> an independent party with expertise in cyber security would be best suited to assess the impact of blocking a particular domain or IP address with a view to protecting public interest, and to decide whether blocking is warranted,

and invites comment on ways to identify "viable, independent parties that may be able to serve as the decision-making authority" accordingly.

76. CIRA submits that the Commission's general view that the impact of assessing blocking, and of deciding when and whether it is warranted, should in each case be made by an independent party with specific expertise, is a key accountability measure required to achieve non-discrimination.

77. This is particularly the case in a market, like Canada's, in which vertical integration between common carriers and content distribution is advanced. Indeed, it is the Commission's long experience with these market realities in the context of the *Broadcasting Act*—notwithstanding early confidence that undue preference rules would beat back the risks of such integration[62]—that led to adoption, first of a *Regulatory framework relating to vertical integration*[63] and then of *The wholesale code,*[64] to help govern the inherent conflicts of interest.

78. However, where the Commission's initial view is that such a role ought to be played by "*an* independent party", CIRA respectfully submits that it is key that any approval framework avoid a single point of failure and all that that implies, including

- regulatory capture risk,
- complacency risk, and
- challenges meeting simultaneous the increasingly diverse needs of TSPs serving commodity consumer, technically savvy, large enterprise, critical infrastructure, consumer or industrial Internet of Things, and other user sectors,

many of which providers may be regulated by sector-specific agencies with their own cybersecurity requirements—consider, for instance, the financial, energy, or railroad sectors.

79. Rather, by focusing on the criteria by which to identify which "viable, independent parties that may be able to serve as [a] decision-making authority", the Commission is in a position to develop an accreditation-based approach similar to those in place, for instance, for domain name registrars,[65]

---

62 *Call for comments on proposed amendments to the Broadcasting Distribution Regulations, Pay Television Regulations, 1990 and Specialty Services Regulations, 1990,* Public Notice CRTC 2000-150, 7 November 2000, paragraph 11 ("[t]he proposed amendments also address the concern that licensees of distributor-affiliated programming services could potentially confer an undue preference on the distributor to which they are affiliated. The proposed amendments therefore introduce a prohibition against pay and specialty services, respectively, granting an undue preference or advantage similar to the provision applicable to distributors by virtue of the Broadcasting Distribution Regulations.").

63 Broadcasting Regulatory Policy CRTC 2011-601, 21 September 2011, and 2011-601-1, 14 October 2011.

64 Broadcasting Regulatory Policy CRTC 2015-438, 24 September 2015.

65 CIRA, "Become a registrar" (online: https://www.cira.ca/ca-domains/sell-ca-domains/become-a-registrar), incorporating the Canadian Presence Requirements, Registrar Agreement (setting out certification requirements and certain registrar obligations), requirement to demonstrate domain knowledge, and other requirements.

independent production funds,[66] or securities trading marketplaces.[67] Criteria should, at minimum, include requisite independence from, and lack of control in fact[68] by, any TSP; technical expertise, as demonstrated by years of activity in this area, by market acceptance, by certifications to well-known ISO or other standards, and by certified endorsement by industry professionals; required program elements, including required mechanisms for accuracy detection and correction and for redress; and such other criteria as should emerge from this proceeding.

D. Defaults (Q5)

Q5. Would botnet traffic be best addressed by default blocking with an option to opt out, or by a model that allows opt-in blocking?

80. The Commission has jurisdiction under section 36 to establish the basis on which it will allow a TSP to block traffic. It does not have jurisdiction absent, perhaps, the exceptional fact-driven circumstances outlined above,[69] to order a TSP to do so. It is therefore unclear that there is a basis to require "default blocking with an option to opt out" in the first place.

81. At the same time, TSPs flooded with malicious traffic have a strong incentive to act to minimize it; would have, under a section 36 approval framework, the capacity to act lawfully to do so, provided it is in a minimally-impairing, proportionate manner; and would therefore have both the incentive and ability to select an opt-out approach on their own, not because the Commission had required it.

82. Accordingly, in our view, the greater concern should be with ensuring that the section 36 approval framework ensures that such blocking is truly necessary and proportionate, including meaningful redress against over-blocking; strong structural safeguards preventing any TSP from making go-it-alone decisions that are prone to abuse; and strict rules that prevent any bleed into content restrictions. A component of this concern is to ensure that users have access to clear information at all meaningful points in the subscriber lifecycle in order to know that they have the ability to opt out, to know and to be able to further investigate what it means to opt out, and to meaningfully exercise their right to opt out without being subjected to unwarranted procedural hurdles.

83. CIRA therefore recommends that, in respect of opting in and out, the Commission ought to ensure that the Internet Code, and such other codes of practice as may be applicable, safeguards users' right to opt out without undue burden.

E. Accuracy (Q6)

Q6. What framework provisions or conditions are required to prevent and mitigate the risks associated with over-blocking and false positives?

---

66 *Policy framework for Certified Independent Production Funds,* Broadcasting Regulatory Policy CRTC 2016-343, 25 August 2016, Appendix.

67 *Marketplace operation,* National Instrument 21-101 (Canadian Securities Administrators), consolidated 14 September 2020; *Trading rules,* National Instrument 23-101 (CSA), consolidated 10 April 2017.

68 The Commission has developed deep experience in this area in applying Canadian ownership and control policies under the *Broadcasting* and, generally, *Telecommunications* Acts. See, *e.g.,* Telecom Regulatory Policy CRTC 2009-428, 20 July 2009.

69 Paragraphs 20-21.

84. CIRA's earlier responses in this intervention have emphasized the importance of transparency reporting, including metrics that report directly on false positives, and of developing a marketplace of accredited actors in order to avoid single points of failure. This competition for accuracy, coupled with the transparency tools for that competition to base itself on ongoing evaluation of the relative accuracy of different list providers, is therefore an important component.

85. At the same time, such reports are worth little if straightforward means to detect over-blocking and false positives are not in place in the first instance. Three elements are therefore fundamental.

86. First, a service standard by which list providers respond to urgent update requests from TSPs, or from trusted third parties, should be a condition of accreditation. Haste and non-ordinary-course emergency response are a key potential vector for over-blocking and false positives. The ability to rely on list providers to move quickly in emergencies is, therefore, an important antidote to situations in which such responses could otherwise arise.

87. Second, a range of methods must be incorporated into the user experience as mandatory elements to be included in the accreditation criteria described at paragraph 79 above, including:

- users' ability to manually look up an IP address or Web site, including their own, to identify whether it has been blocked, and any surrounding metadata as to why, including archival requirements;
- an appropriate interface to such lists and archives, such as a RESTful API, by which third parties could develop tools for more targeted testing, subject to any anti-abuse terms;
- prompt notices to overblocked sites, who would have the ability and incentive to publicize such overblocking, generating commercial pressure on the list provider to improve accuracy; and
- a root-cause-analysis obligation on the TSP (who would liaise with list providers), including a service standard for timeliness, in order to ensure fundamental redress.

88. Third, we note that an FCC CSRIC best practice recommends that service providers "ensure that detection methods do not block legitimate traffic in the course of conducting botnet detection, and should instead employ detection methods which seek to be non-disruptive and transparent to their customers and their customers' applications."[70]

89. To address this concern that pertains to the TSP's implementation of a blocklist from a certified provider, rather than to the accuracy of the certified provider's list itself, the section 36 approval framework establishing the conditions under which a TSP could undertake botnet-related traffic blocking should:

- require TSPs to log in machine-readable format, in a trusted manner that meets integrity requirements, both blocked identifiers and the frequency of their blocking;
- require TSPs to file such logs with list providers who would in turn, as a component of their service based on conditions of certification, run a compare to flag any entries not drawn from their own blocklists, shipping the compare to the Commission's enforcement team or a Commission-designated intermediary for consolidation and identification of sites that may have been overblocked or improperly blocked; and
- require reporting from the TSP on identifiers listed on the compare, and on which the Commission's enforcement team could follow up.

---

[70] FCC CSRIC Best Practices, note 50 above, Item 12-8-8915.

This approach would create a mechanism to detect, and remediate, both TSP error and TSP blocking improperly initiated of the TSP's own accord.

F. Technical Design (Q8, Q9, Q10)

Q8. Which network-level blocking techniques are best suited to stop or limit botnet communication?

90. The approach recommended in this intervention focuses on establishing sufficient transparency, accountability, and single-point-of-failure avoidance, so as to create the conditions for competition to emerge in respect of the techniques that will be most effective. It has, similarly, focused on ecosystem interoperability through APIs, mark-up formats for automated notifications, and so forth.

91. CIRA respectfully submits that such an ecosystem-focused approach that coheres through information exchange, rather than the one-true-technique focus implied by Q8, is more consistent with cybersecurity best practices in relation to malicious traffic such as botnets:

> Service Providers should make reasonable efforts to communicate with other operators and security software providers, by sending and/or receiving abuse reports via manual or automated methods. These efforts could include information such as implementation of "protective measures" such as reporting abuse (e.g., spam) via feedback loops (FBLs) using standard message formats such as Abuse Reporting Format (ARF). Where feasible, ISPs should engage in efforts with other industry participants and other members of the internet ecosystem toward the goal of implementing more robust, standardized information sharing in the area of botnet detection between private sector providers.[71]

92. It is also essential to this ecosystem diversity that TSPs have, and that end-users continue to have, the ability to select between the legitimate provider of their choice—not just as a basic principle of net neutrality, but also as a means of ensuring endpoint security. To that end, we note that CSTAC's Security Best Practice draft endorses, as a best security practice, that "[o]rganizations should enable subscriber[s] to select and route DNS request[s] to resolvers of their choice".[72]

93. In view of the importance to security diversity of ensuring that end-users have and know that they have such choices, we suggest that a cybersecurity lens be applied to any allegation that an ISP blocks end-user access to domain resolvers or protocols not clearly both specified and justified in its disclosures in a manner consonant with the section 36 approval framework to be developed. Failure to do so would be a presumptive undue disadvantage under subsection 27(2) of the *Telecommunications Act.*

Q9. If domain-based blocking is identified as a preferred technique, which domain resolver selection considerations would a blocking framework need to take into account?

94. A robust international market has emerged in privacy- and security-protective domain resolvers that are independent of TSPs. CIRA is the operator of such domain resolvers, as identified at paragraph 42 of the Notice, and on which many Canadian consumer and enterprise users choose to rely to assist in their cybersecurity posture and safe internet usage.

95. We agree that domain resolvers already play, and can play in the hands of the TSPs who are the objects of this proceeding, an important role in reducing harms to the Canadian internet. Canadian internet

---

71 FCC CSRIC Best Practices, note 50 above, Item 12-8-8912.

72 *Security Best Practice for CTSPs,* note 29 above, at section 3.2.3.17 (entitled "DNS—Net Neutrality").

users' ability to select between the legitimate intermediaries of their choice, including domain resolvers, is a fundamental to a robust and resilient cybersecurity ecosystem for the reasons set out above.

96. The DNS services of these resolvers are not "basic telecommunications services", do not "allow individuals to engage autonomously in two-way voice telecommunications or to access the Interent autonomously", and are not rendered TSPs by the provision of these services.[73] However, TSPs bundle default DNS into their internet connectivity services—and an ISP's incorporation into its connectivity services of DNS resolvers that block traffic is an activity that requires section 36 approval. Indeed, a growing number of TSPs similarly rely, directly or indirectly, on related third-party services in order to provide internet connectivity to users and to endpoints.

97. Because they receive, process, and return DNS resolution requests, third-party domain resolvers are exposed to sensitive information about end-user traffic patterns, including:

a) every domain name whose resolution an endpoint requests, and
b) the unique identifier associated with that endpoint.

In other words, domain resolvers can be privy to every site that a subscriber visits on the Internet.

98. This is exactly the kind of personal information in which Canadians' privacy interests attract constitutional protections that are of "a higher standard than that available under PIPEDA."[74] It is also the kind of personal information about which Canadian internet users have deep concerns regarding cross-border exposure.[75]

99. Mindful of these risks and of the constitutional and statutory protections that any section 36 approval framework must meet in addressing them, including those provided by paragraphs 7(e) and (i) of the *Telecommunications Act,*[76] CIRA suggests as follows. Default domain resolvers that block traffic and are incorporated into basic telecommunications services, such as the internet connectivity that TSPs provide to the public, ought to have been audited by an independent third party, and to have deposited such audit with the contracting TSP and with the Commission, to basic standards in respect of privacy, cybersecurity, and participation in Canada's cybersecurity ecosystem, including:

- resiliency, disaster recovery, and compromise and corruption remediation procedures within a robust cybersecurity framework,[77] including monitoring and query logging associated with

---

73 *Telecommunications Act,* note 7 above, subsection 2(1) (definition of "telecommunications service provider"), with reference to *Enhanced services,* Telecom Decision CRTC 84-18, section C.1 (definition of "basic service"); *Review of the reseller registration obligation,* Telecom Regulatory Policy CRTC 2019-354, 24 October 2019.

74 *R. v. Spencer,* 2014 SCC 43; above, notes 41 and 44 and accompanying text.

75 *Canadians Deserve a Better Internet,* note 34 above.

76 Note 7, above. Paragraph 7(e) requires the Commission to exercise its powers with a view to promoting "the use of Canadian transmission facilities for telecommunications within Canada and between Canada and points outside Canada." Paragraph 7(i) requires approaches that "contribute to the protection of the privacy of persons".

77 CSTAC Best Practice, note 29 above, sections 3.2.2 ("DNS Hardening and Security"), 3.2.3 ("DNS Service Protection Overview"), and 3.2.3.6 ("Resiliency Across DNS Service"); FCC CSRIC Best Practices, note 50 above, items 12-12-8046 (general compromise protection), 12-12-8047 (DNS resiliency), 12-12-8117 and 12-12-8527 (disaster recovery), 12-12-8528 (attack responses), 12-8-8903 (anti-spoofing)

meaningful anomaly and attack detection[78] and mitigation measures for cache poisoning and stretching, including DNSSEC implementation;[79]

- internal privacy protection and encryption,[80] including best data and retention period minimization, pseudonymization, and encryption at rest and in transit (including DoT/DoH implementation, as updated);

- privacy supply chain measures, including in-country data residency and presence at major public Internet exchanges;

- accountability indicators, like transparency reporting and completeness and comprehensibility of privacy policies; and

- participation in both industry-wide and Canadian telecommunications cybersecurity information and threat exchange forums and initiaives, including reputable DNS block lists and other similar tools that meet transparency and certification requirements.[81]

100. In CIRA's view, and in keeping with the approach put forward generally in this submission, a systemic approach that focuses on the standards to be met and certifications to assure them, rather than designation of "particular domain resolvers", is the better approach in this regard.

Q10. How should technology changes be addressed in the network-level blocking framework?

101. The ecosystem-focused approach described above would lend itself well to adapting to technology changes in a way that a centrally-administered, single-point-of-failure approach is unlikely to:

> The mitigation of botnets requires a thoughtful, holistic approach. The various parts of this complex ecosystem must — for their individual and collective good — deepen and sharpen their understanding of their own responsibilities and how they complement those of others. And in cases where the lines currently are unclear or unknown, stakeholders must work together to clarify them. Absent such work, strategies for combating botnets will revert to the fallacy of utopian solutions focused on just one or two pieces of the puzzle — for instance, that ISPs should simply shut down all botnets, or that billions of devices should be made universally secure, or that consumers should become omniscient users of technology.[82]

---

78 CSTAC Best Practice, note 29 above, sections 3.2.3.7 ("DNS Monitoring"), 3.2.3.11 ("DNS Query Logging"), and 3.2.3.14 ("DNS – Detection and Defence") ; FCC CSRIC Best Practices, note 50 above, item 12-12-8048 (DDoS protection)

79 CSTAC Best Practice, note 29 above, sections 3.2.3.12 ("DNS Cache Poisoning") and 3.2.3.13 ("DNS Cache Stretching"); FCC CSRIC Best Practices, note 50 above, item 12-12-8048 (cache poisoning) and 12-8-8904 (DNSSEC).

80 CSTAC Best Practice, note 29 above, sections 3.2.3.15 ("DNS - Privacy Protection"), 3.2.3.16 ("DNS – Cryptography Security").

81 FCC CSRIC Best Practices, note 50 above, items 12-12-8908 and 12-12-8909 (DNS block lsits that are made generally available, such as via a public website).

82 Council to Secure the Digital Economy, *International Botnet and IoT Security Guide 2020* (Washington, DC), page 17. (The CSDE is the joint project of USTelecom, the wireline carrier trade association, and the Consumer Technology Association ("**CTA**"), well-known for the annual Consumer Electronics Show it convenes in Las Vegas each January.)

102. Generally, we have sought to outline an approach to developing a safe marketplace that avoids single points of failure. A resilient approach to malicious traffic detection and remediation is one that will help foster a rich and complete ecosystem, including the role of TSPs within it, that respects the principles of transparency, non-discrimination, necessity, and proportionality. The information interchange, cooperation, competition, and metrics approaches described in this intervention are key elements of such an ecosystem.

G. Conclusion

103. The approach set out in this intervention underlines the Commission's limited jurisdiction in the area of network security, alongside its fundamental responsibilities for safeguarding net neutrality, as a form of common carriage, for protecting the privacy of persons, and for promoting competition.

104. To that end, CIRA's intervention has sought to delineate an approval framework around purely network-integrity-focused measures in a way that subjects blocking activities that likely already occur, whether or not lawful, to independent oversight designed to prevent such blocking from offending net neutrality, privacy, or provider choice.

105. To do so, the intervention has emphasizesd four principles (transparency, non-discrimination, necessity, and proportionality) that CIRA submits ought to be fundamental to such a blocking approval framework, as they have been in respect of the Commission's traffic management approval framework. It has developed, based on these principles, an ecosystem-focused approach that fosters competition, informed users and providers, and an avoidance of single points of failure at each stage. Most importantly, it has provided guidance on a framework that:

- is practical, workable, but laser-focused on technical threats that weaponize the internet itself such that failing to remediate them threatens the ability to use the internet, and
- cannot be used to block content or online speech—a remedy that is rarely necessary, generally disproportionate and, if not held at arm's-length to the technical matters canvassed in this proceeding, the beginning of a slippery slope to kill switches that threaten the ethos of the internet and are fundamentally at odds with the Government of Canada's and the CRTC's commitments.

106. CIRA thanks the Commission for considering these submissions, and looks forward to reviewing the interventions of other parties.

Yours sincerely,

[filed electronically]

Byron Holland
President & Chief Executive Officer

*** End of Document ***