Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes

Compliance and Enforcement and Telecom Decision CRTC 2026-140

PDF version

Gatineau, 18 June 2026

Public record: 1011-NOC2025-0143

Expansion of network-level blocking framework

Summary

The Commission helps ensure that Canadians have access to safe and reliable telecommunications services through its work under the *Telecommunications Act* (the Act) and Canada's Anti-Spam Legislation (CASL). Under the Act, the Commission plays a narrow role by promoting compliance with the Unsolicited Telecommunications Rules to help prevent Canadians from receiving unwanted calls that do not comply with those rules. Under CASL, the Commission helps protect Canadians from online spam, along with the Competition Bureau and the Office of the Privacy Commissioner, by promoting and monitoring compliance within a civil regulatory regime.

Botnets are networks of computers, cellphones, or other devices that have been infected with malware. This allows individuals or groups to control the devices without the knowledge or consent of their owners. Botnets can be used for sending spam to Canadians or for other harmful activities.

Network-level blocking can help disrupt botnets. It plays a critical role in helping TSPs protect Canadians from fraud, scams, and other harmful activities. This includes helping prevent people from receiving emails or text messages designed to trick them into sharing their personal information with individuals or groups who intend to misuse it.

In Compliance Enforcement and Telecom Decision 2025-142, the Commission established a framework to allow Canadian carriers to block botnets or other harmful activities within their networks before reaching Canadians' devices. The Commission then launched a consultation to gather views on whether the framework should be expanded.

The Commission heard from a wide range of participants during the proceeding, including the National Cybercrime Coordination Centre of the Royal Canadian Mounted Police, the Independent Telecommunications Providers Association, and several carriers. Based on the public record, the Commission is expanding the network-level blocking framework to allow Canadian carriers to use any approved blocking method that complies with the framework's guiding principles of necessity, accuracy, and consumer privacy. Blocking must be done in accordance with the blocking framework set out in the appendix to this decision, starting on 18 June 2026. In addition to providing more flexibility to carriers who engage in network-level blocking, this decision simplifies the framework's requirements for reporting to the Commission and sharing information with the public.

Canada

The revised framework aims to help minimize administrative burden on TSPs, lower compliance costs, and promote innovation, while helping TSPs more effectively protect Canadians from fraud, scams, and other harmful activities.

A dissenting opinion by Commissioner Bram Abramson is attached to this decision.

Background

1. In Compliance and Enforcement and Telecom Decision 2022-170, the Commission determined that the most appropriate regulatory approach to address botnets[1] was to create a framework guided by the principles of necessity, customer privacy, accountability, transparency, and accuracy. This framework sets out the terms and conditions under which Canadian carriers may engage in network-level blocking.

2. In Compliance and Enforcement and Telecom Decision 2025-142, the Commission established a framework authorizing carriers to block botnets and other harmful activities within their networks using blocklists[2] that meet specified criteria. At the same time, the Commission initiated a proceeding through Compliance and Enforcement and Telecom Notice of Consultation 2025-143 (the proceeding) to consider whether the framework should be expanded to include other blocking methods and, if so, whether additional privacy safeguards and reporting requirements are needed.

3. The Commission received interventions from the Independent Telecommunications Providers Association, the National Cybercrime Coordination Centre (NC3) of the Royal Canadian Mounted Police, and eight carriers: Bragg Communications Inc., carrying on business as Eastlink (Eastlink), Bell Canada, Cogeco Communications Inc. (Cogeco), Quebecor Media Inc. (Quebecor), Rogers Communications Canada Inc. (Rogers), Saskatchewan Telecommunications, TekSavvy Solutions Inc., and TELUS Communications Inc. (TELUS). Bell Canada, Rogers, and TELUS also provided replies to interventions.

Issues

4. The Commission has identified the following issues to be addressed:

    - Should the scope of the framework be expanded to include blocking methods other than

---

[1] Botnets are networks of computers, cellphones, or other devices that have been infected with malware. This allows individuals or groups to control the devices without the knowledge or consent of their owners. Botnets can be used for sending spam to Canadians or for other harmful activities.

[2] Blocklists are lists of indicators of compromise that help identify harmful activity. Carriers use these lists to block suspicious or dangerous online traffic from passing through their networks.

blocklists?

- Should the framework include additional safeguards to protect privacy?
- Should the reporting requirements of the framework be revised?

Should the scope of the framework be expanded to include blocking methods other than blocklists?

Positions of parties

5. Carriers indicated that they rely on a range of blocking methods other than blocklists to block botnets and other cyber threats, including port blocking,[3] blocking forged source addresses,[4] and blocking traffic based on volume anomalies.[5]

6. Most carriers cautioned that any expansion of the framework must allow carriers flexibility to address the dynamic nature of botnets and other cyber threats. They stressed that carriers require independence and operational discretion to implement and adapt their blocking methods, sometimes in real time, in response to rapidly evolving threats. The NC3 reinforced this point by emphasizing that network-level threats are becoming more sophisticated and covert, and are increasing in scale, speed, and precision.

7. Some carriers also suggested that a framework that only allows certain blocking methods and prescribes strict conditions of use will be ineffective and potentially counter-productive. Bell Canada noted that, under the current framework, a carrier can only use third-party blocklists if they meet a long list of criteria that vendors may not be able or willing to comply with. This could force carriers to stop using third-party blocklists, undermining the very network security the framework is intended to promote.

8. TELUS submitted that the framework's current complaint resolution requirements would not be feasible if more blocking methods are incorporated into the framework.

---

[3] Port blocking is the practice of blocking Internet traffic from using specific communication ports that are known to be targets for malicious activity. Carriers block selected ports to protect users from attacks that commonly exploit these ports.

[4] Forged source addresses are Internet Protocol (IP) addresses that have been modified to hide the identity of the sender and make the receiving system believe the traffic came from a trusted or different source. Blocking Internet traffic with forged addresses helps carriers prevent attacks that rely on impersonating legitimate users or systems.

[5] Traffic volume anomalies refer to unusual changes in the amount of data flowing through a network. Carriers monitor and block traffic volume anomalies to keep networks stable and protect against cyber attacks.

Commission's analysis

Blocking methods

9. Carriers combine various blocking methods to protect their networks, including blocklists, port blocking, blocking forged source addresses, and blocking traffic based on volume anomalies. These methods are well established and align with industry-recognized best practices developed by the Canadian Security Telecommunications Advisory Committee (CSTAC) and the Internet Engineering Task Force.[6]

10. Limiting the framework could result in carriers blocking malicious traffic without Commission authorization or restricting their ability to respond to emerging harmful activities. While a centralized and prescriptive model might make implementation more consistent, it could force carriers to stop using blocking methods that are widely used and aligned with industry best practices. It is also likely to be ineffective, as any attempt to specify solutions in advance will be outpaced by constantly evolving harmful activities.

11. Adopting a simple, principles-based regulatory model will support carriers' existing blocking practices while granting them discretion to make choices about tools, vendors, and implementation details. Consistent with the 2023 Policy Direction,[7] this model will encourage carriers to compete and innovate as technologies evolve and malicious actors use new tactics.

12. Given that carriers use various blocking methods and that there is broad agreement on the need for flexibility to address emerging harmful activities, the Commission will expand the framework to permit any blocking method that complies with the principles of necessity, accuracy, and consumer privacy. These principles emphasize that blocking under the framework must be done exclusively for the purpose of cyber security, that any impact on legitimate services must be limited to what is necessary to block the malicious traffic, and that consumer privacy must be fully safeguarded.

Complaint resolution

13. The principle of accuracy established in Compliance and Enforcement and Telecom Decision 2022-170 and set out in section 5 of the current framework states that the public must have the opportunity to report and resolve false positives and over-blocking in an effective and

---

[6] CSTAC is an advisory committee that allows the private and public sectors to exchange information and collaborate strategically on current and evolving issues that may affect telecommunications infrastructure, including cyber security threats. CSTAC includes the Canadian Telecommunications Cyber Protection Working Group, which has developed best practices for Canadian telecommunications service providers. The Internet Engineering Task Force is an international body that develops standards for the IP suite, namely Transmission Control Protocol/Internet Protocol (TCP/IP).

[7] *Order Issuing a Direction to the CRTC on a Renewed Approach to Telecommunications Policy,* SOR/2023-23, 10 February 2023, subsections 2(a) and (f).

timely manner. However, it does not prescribe fixed timelines or specific carrier actions.

14. The current framework requires carriers to resolve customer complaints within two business days by either updating the relevant blocklist or reporting back to the customer.

15. The record of the proceeding suggests that these requirements may be impractical given the operational steps carriers must take to resolve complaints and the various blocking methods and vendor solutions in use. Moreover, the current requirements apply only to complaints related to blocklists.

16. Therefore, the Commission will require carriers to resolve complaints within five business days without mandating the specific actions they must take. This approach ensures customers have access to a timely remedy while recognizing that complaint investigations can be complex, resource-intensive, and dependent on third-party cooperation.

17. In light of the above, the Commission determines that the framework will be revised to:

    - allow carriers to use any blocking method consistent with the framework's guiding principles; and

    - provide carriers more flexibility in how they resolve customer complaints.

18. The definitions of "blocklist" and "blocklist provider" in the previous framework have been replaced with the broader definitions of "blocking method" and "third-party provider" to reflect the expanded scope of the framework.

Should the framework include additional safeguards to protect privacy?

Positions of parties

19. Most carriers submitted that no additional privacy safeguards are needed, as existing privacy laws and Commission rules and regulations already protect Canadians and their personal information in the context of network-level blocking.

20. Carriers generally agreed that the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the Commission's own consumer confidentiality safeguards[8] provide sufficient privacy protections. Quebecor submitted that imposing new prohibitions on the use of personal information collected under the framework could hinder innovation, undermine the effectiveness of cyber security measures, and prevent the development of tools that benefit consumers. Cogeco

---

[8] In addition to PIPEDA, carriers are required to comply with consumer confidentiality safeguards imposed by the Commission (see for example Telecom Decision 2003-33; Telecom Regulatory Policies 2009-723 and 2017-11; and Telecom Decision 2022-238).

submitted that new prohibitions could conflict with exceptions and exemptions under existing privacy laws.

21. While most carriers reported that personal information collected under the framework is used only for blocking purposes, Quebecor and TELUS suggested that certain secondary uses, including marketing, should be permitted if conducted in compliance with applicable laws and regulations. TELUS noted that the Office of the Privacy Commissioner of Canada has recognized that online behavioural advertising may be considered a reasonable purpose under PIPEDA, provided it is carried out under certain parameters.[9]

Commission's analysis

22. In Compliance and Enforcement and Telecom Decision 2022-170, the Commission made consumer privacy a guiding principle of the framework. This principle was subsequently given effect in section 8.2 of the framework published in Compliance and Enforcement and Telecom Decision 2025-142. Carriers are expected to comply with existing privacy obligations and adopt best practices to provide the highest level of protection. This means ensuring that personal information collected, used, or disclosed for blocking is limited to what is essential for that purpose, only for so long as it is necessary for that purpose, and not used or disclosed for any other purpose.

23. Carriers are generally meeting the framework's consumer privacy expectations. Carriers appear to restrict the collection, use, and disclosure of personal information to what is necessary for blocking purposes, retain it only for short periods, and anonymize and aggregate it once blocking activities are complete. Access is limited to authorized personnel, and disclosures are made only where required by law.

24. In light of the above, the Commission determines that no additional privacy safeguards are needed beyond those already established in the framework. The Commission does, however, consider it appropriate to clarify, as reflected in section 7.3 of the framework set out in the appendix to this decision, that any use of deep packet inspection[10] must be limited to exceptional circumstances such as compliance with a court order or fine-tuning threat management systems following a cyber attack. In such cases, inspection must be limited to packet headers and must not involve inspection of the content of communications.

25. With respect to the suggestion that personal information collected under the framework could be used for secondary purposes, the Commission considers, as reflected in section 7.2 of the framework set out in the appendix to this decision, that the guiding principle of consumer privacy

---

[9] *Office of the Privacy Commissioner of Canada* (2015), Policy position on online behavioural advertising.

[10] Deep packet inspection is a method of examining the content of data packets that pass through a network. It can be used to detect packets with malicious content.

is intended to be flexible to accommodate lawful, consent-based, or otherwise authorized secondary uses.

Should the reporting requirements of the framework be revised?

Positions of parties

26. Most carriers raised concerns about the framework's current reporting requirements.

27. Many carriers warned that detailed public reporting of carriers' blocking practices and performance could indirectly help malicious actors identify potential vulnerabilities, tailor attacks, and bypass network-security protections.

28. Some carriers raised doubts about the value to consumers of technical information regarding the network-level blocking solutions applied by carriers. They suggested that the average Canadian is not likely to be interested in the information reported or fully understand it.

29. Several carriers also submitted that it would be complicated and resource intensive to build and retool their systems to comply with the reporting requirements. They noted that blocking solutions are not typically designed to provide detailed reporting data. TELUS and Eastlink suggested that such technical limitations may prevent carriers from being able to comply with the reporting requirements.

30. Bell Canada recommended that the Commission ask the CRTC Interconnection Steering Committee (CISC) Network Working Group (NTWG)[11] to re-examine the issue of appropriate reporting metrics. In the alternative, Bell Canada suggested that the current reporting requirements be replaced by the two metrics suggested by the CISC NTWG in the report considered in Compliance and Enforcement and Telecom Decision 2025-142: the number of indicators of compromise (IOCs) blocked and the number of false positives reported. As a further alternative, Bell Canada suggested reducing and clarifying existing reporting rules and letting carriers file their reports in confidence.

Commission's analysis

31. In Compliance and Enforcement and Telecom Decision 2022-170, the Commission made transparency a guiding principle of the framework and established the following:

    - Carriers are expected to share enough information on their websites about their blocking solutions to allow customers to make informed decisions about which carriers they want

---

[11] The CISC is an organization established by the Commission to assist in developing information, procedures and guidelines as may be required in various aspects of the Commission's regulatory activities. The NTWG undertakes tasks related to network operations and issues.

to do business with, but not so much that it would help malicious actors bypass those solutions.

- Carriers are expected to report performance metrics to the Commission to allow for public disclosure of aggregate statistics and assessment of whether further regulatory action is needed.

32. This principle was subsequently given effect in sections 6 and 7 of the framework published in Compliance and Enforcement and Telecom Decision 2025-142.

Information on carrier websites

33. The Commission considers that general information on carrier websites about blocking practices is adequate to support consumer choice. The Commission further considers that requiring advance public notice for every change to a blocking method could alert malicious actors and undermine the framework's effectiveness.

34. Therefore, the Commission will revise the framework to require carriers to publish fewer technical details on their websites, while ensuring that carriers publicly disclose enough information about their blocking practices to help customers make informed decisions. This will reduce the administrative burden on carriers and the risk of exposing sensitive information to malicious actors, while ensuring a baseline level of transparency of carriers' blocking activities.

Reporting to the Commission

35. The Commission notes that, under the current framework, reporting requirements are much more detailed than what the two metrics recommended by the CISC NTWG provide (unique IOCs blocked and false positives reported). These metrics were identified by the industry as sufficient to provide meaningful insight into carrier performance. The Commission considers that limiting requirements to these metrics would help reduce compliance costs for carriers.

36. However, the Commission considers that it requires more information than these two metrics provide to exercise effective oversight. While the number of IOCs blocked and false positives received provides a basic indication of the scope of blocking and its impact on legitimate services, they do not offer enough information to assess whether carriers' blocking practices are consistent with the framework's guiding principles. Limiting reporting requirements addresses concerns raised about regulatory burden, but it also removes important indicators of carrier blocking activity and performance.

37. The new regulatory model is also not as prescriptive as the original approach, which relied on detailed technical criteria to ensure compliance with terms and conditions. Under the new approach, carriers have more flexibility in choosing blocking methods and operational details. As a result, the Commission considers that, under the revised framework, carriers must adjust how they demonstrate accountability.

38. Considering the simplified requirements of the revised framework, the Commission determines that carriers will be required to submit streamlined annual reports to the Commission. The report must include the following:

    - the total number of IOCs blocked by the carrier;
    - the total number of false-positive and over-blocking complaints received from customers;
    - a description of the network-level blocking measures used; and
    - an explanation of how the blocking measures comply with the framework.

39. This approach will enable effective oversight while protecting sensitive information and allowing carriers flexibility to demonstrate compliance in ways that reflect their unique network environment. It will also give the Commission the information it needs to identify potential concerns (e.g., high-risk vendors, privacy-invasive tools, and over-blocking risks) and verify compliance. Where necessary, the Commission may take measures to address non-compliance, including requesting additional information, engaging with carriers to clarify or adjust practices, or using other investigation and enforcement tools under the *Telecommunications Act* (the Act).

40. To enhance public transparency, the Commission will, at its discretion, make public the number of IOCs blocked and the number of false-positive or over-blocking complaints reported, since these are unlikely to be exploited by malicious actors. The Commission also intends to use the information submitted in confidential annual reports to develop aggregated summaries of blocking activities across the industry. These summaries will explain the scope, impact, and benefits of carrier blocking activities in a way that is accessible and meaningful to Canadians, while protecting sensitive information.

41. The Commission considers that this approach strikes the right balance between transparency to the public, accountability, and confidentiality of carriers' blocking practices.

Conclusion

42. The Commission approves, in accordance with section 36 of the Act, the revised framework for network-level blocking set out in the appendix to this decision. It will take effect on 18 June 2026.

43. Under section 36 of the Act, Canadian carriers require Commission approval to control or influence the content of telecommunications. By blocking botnet traffic and other harmful activities, Canadian carriers may prevent the delivery of telecommunications to users, thus controlling the content of the telecommunications they carry for the public. Accordingly, such activity falls within the scope of section 36 of the Act.

44. The framework sets out the terms and conditions that allow Canadian carriers to block botnets

and other harmful activities. Participation in this framework is voluntary; carriers are not required to block Internet traffic crossing their networks to protect against cyber attacks. However, if they choose to do so, they must comply with the terms and conditions set out in the framework.

45. The Commission encourages non-carrier telecommunications service providers (TSPs) to adopt a similar approach. If non-carrier TSPs choose to block network traffic for cyber security purposes in a manner that is inconsistent with the framework, the Commission may consider whether further regulatory action is needed.

2023 Policy Direction

46. The Commission considers that the framework will advance the telecommunications policy objectives set out in the Act[12] as well as the consumer interests and innovation objectives of the 2023 Policy Direction by helping protect Canadians from botnets and other harmful activities and making telecommunications services more reliable. The framework is designed to be technologically neutral and flexible to encourage innovation by carriers in addressing online harms, and to help protect the privacy of persons by prohibiting unauthorized access to and collection of their personal information.

Secretary General

[12] The relevant objectives are: 7(b) to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada, (g) to stimulate research and development in Canada in the field of telecommunications and to encourage innovation in the provision of telecommunications services, (h) to respond to the economic and social requirements of users of telecommunications services, and (i) to contribute to the protection of the privacy of persons.

Appendix to Compliance and Enforcement and Telecom Decision CRTC 2026-140

Framework for network-level blocking

Definitions

Blocking method: Any measure that may be used by a carrier to block malicious Internet traffic traversing their network.

Canadian carrier (as defined in the *Telecommunications Act*): A person who owns or operates a transmission facility used by that person or another person to provide telecommunications services to the public for compensation.

Customer: A person who subscribes to the carrier's services that are subject to the blocking.

Cyber attack: Malicious use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

Cyber security: A body of technologies, processes, practices, and response and mitigation measures designed to protect against cyber attacks in order to ensure confidentiality, integrity, and availability of electronic information.

False positive: Occurs when non-malicious content is incorrectly blocked.

Indicator of compromise (IOC): An identifier used by carriers to block network traffic for cyber security purposes that indicates, with a high degree of confidence, intrusion on a system and that malicious activity is occurring. In other words, an IOC is a technical characteristic of a particular cyber attack.

Over-blocking: Blocking applied to malicious traffic in an overly broad manner or to benign content.

Reporting period: The calendar year from 1 January to 31 December (12 months), with the first reporting period beginning on the day that the framework set out in the appendix to Compliance and Enforcement and Telecom Decision CRTC 2026-140 comes into effect and ending on 31 December of that year.

Third-party provider: Any person or entity that supplies systems, equipment, or software that a carrier uses to implement a blocking method.

***

Pursuant to section 36 of the *Telecommunications Act,* the Commission authorizes Canadian carriers to take cyber security measures to block Internet traffic traversing their networks, solely for the

purpose of protecting against cyber attacks, subject to compliance with the terms and conditions set out below. The terms and conditions will come into effect on 18 June 2026.

This authorization does not apply to the blocking of traffic for any other purpose, including blocking otherwise illegal activity, or blocking for commercial, competitive, or political purposes.

1.0. Blocking by default

1.1. Blocking must operate at the network level by default: a customer cannot opt in or opt out.

1.2. The carrier must not, however, implement any measure that may prevent customers from employing legitimate services that may circumvent the blocking, such as virtual private network services or alternative Domain Name System resolvers.

2.0. Authorized blocking measures

2.1. The carrier may only block malicious Internet traffic using measures that comply with the guiding principles of necessity, accuracy and consumer privacy set out in Appendix 1 to Compliance and Enforcement and Telecom Decision CRTC 2022-170.

2.2. The onus is on the carrier to demonstrate that its measures are consistent with these principles, as set out in paragraph 6.1(d) of this framework.

2.3. Third-party providers used by a carrier must meet, at a minimum, the following criteria:

(a) The third-party provider has the necessary technical expertise, as demonstrated, for example, by years of activity in researching new and changing cyber threats, by market acceptance and certified endorsement of industry professionals, or by certifications to well-known international standards.

(b) The third-party provider has no potential conflicts of interest (e.g., ownership and geopolitical context) that may compromise the operation of its systems, equipment, or software in an unbiased manner and in the best interests of Canadians.

3.0. Necessity

3.1. A carrier may only use a blocking method for the purpose of protecting their networks and customers' computers from malicious botnets (i.e., from joining a network of malware-infected devices controlled by a threat actor without the customers' knowledge and consent) and from other cyber threats, including malware and phishing.

4.0. Accuracy

4.1. A carrier must ensure that its blocking methods are accurate and minimize the risk of false positives and over-blocking.

4.2. A carrier should take steps to limit the impact of its blocking activities on legitimate services to what is necessary to block the malicious traffic. This may include mechanisms to verify that the blocked traffic is malicious, processes to assess potential collateral damage on legitimate services, and procedures to update or refine blocking methods.

4.3. A carrier must have a process in place for receiving, validating, and resolving customer complaints related to false positives and over-blocking.[1] This process should include reviewing the reported issue, adjusting or updating the blocking method as needed, and notifying the customer as needed.

4.4. The carrier must resolve a complaint within five business days of its receipt.

5.0. Transparency (public disclosure)

5.1. The carrier must disclose, clearly and prominently on its website, information about the cyber security blocking occurring under this framework. This information must be identified with a distinct "cyber security blocking" heading.[2] The carrier must also reference its online disclosures in relevant marketing materials, customer contracts, and terms of service.

5.2. The online disclosure must provide (i) sufficient, plain-language information for Canadians to understand the type and scope of blocking that is in place, (ii) whether the carrier relies on third-party providers to support its blocking activities (including whether any such providers are located outside of Canada), (iii) the process for filing and investigating complaints related to potential false positives and over-blocking, and (iv) any relevant privacy-related information and necessary statements. At a minimum, the following information should be included:

(a) That the blocking follows the terms and conditions set out in this framework.

(b) A general description of the blocking methods in use and how they work.

(c) The carrier's contact information for filing complaints and the process that will be followed.

(d) That the blocking aims to provide a safer Internet service, but it is not a replacement for user-level protections: service providers provide cyber security protections for their networks and customers provide cyber security protections for their own devices. Therefore, it is important that customers continue to secure their devices and their

---

[1] Customers may also submit complaints directly to the Commission through the Contact us page.

[2] This information may be published on the same webpage as the information disclosed pursuant to the Commission's existing requirements related to Internet traffic management practices or at any other relevant location.

Internet connection against cyber threats (e.g., by installing and updating antivirus software, performing regular software updates, managing a firewall, using strong passwords, enabling two-factor authentication, and securing their wireless connection).

5.3. Online disclosure is to be made accessible for persons with disabilities in a manner consistent with the accessibility determinations outlined in Broadcasting and Telecom Regulatory Policy CRTC 2009-430.

6.0. Transparency (Commission reporting)

6.1. The carrier must file in confidence with the Commission[3] the following information regarding its blocking activities over the reporting period, within 30 calendar days of the end of each reporting period:[4]

(a) Identification of all the blocking methods used by the carrier, including any third-party providers or products relied upon.

(b) The total number of IOCs blocked by the carrier.

(c) The total number of false-positive and over-blocking complaints received from customers.

(d) Detailed rationale explaining how the blocking complies with the terms and conditions of this framework.

(e) A hyperlink to the webpage used to meet the disclosure requirements set out in section 5.0.

7.0. Accountability and privacy

7.1. The carrier must periodically review all its blocking systems subject to this framework to verify that they work as intended.

7.2. If the carrier collects, uses, or intends to disclose personal information for the purpose of the activities performed under this framework, the carrier must fully comply with all applicable laws and regulations pertaining to the protection of personal information. This framework does not permit any additional collection, use, or disclosure of personal information, except where such activities are authorized by applicable laws and regulations or by an order from a

---

[3] Regarding the submission method, refer to the webpage Submitting applications and other documents to the CRTC using My CRTC Account.

[4] The Commission may, at its discretion, make the metrics reported in (b) and (c) publicly available. The Commission may also use the information from confidential annual reports to develop aggregated summaries of network-level blocking activities across the industry.

court of competent jurisdiction.

7.3. Any use of deep packet inspection under this framework must be limited to exceptional circumstances, such as compliance with a court order or fine-tuning threat management systems following a cyber attack. In such cases, inspection must be limited to packet headers and must not involve inspection of the content of communications.

8.0. Other conditions

8.1. The carrier must comply with any other conditions that the Commission may establish from time to time following a public process.

Dissenting opinion of Commissioner Bram Abramson

1. The *Telecommunications Act* (the Act) prohibits carriers from controlling the content or influencing the meaning or purpose of telecommunications they carry for the public unless the Commission approves otherwise. The existing framework approved network-level blocking of botnet traffic. The revised framework approves more and oversees less: less disclosure, less structured complaint handling, less privacy protection. Carrier discretion has expanded. Governance of that discretion has contracted.

2. That inversion is why I dissent. The consequence is not abstract. Where lawful communications are wrongly blocked or sensitive traffic observed and repurposed, no one will be positioned to notice, and no one overseeing the system obliged to find out. I agree with the majority that the framework for approved botnet-level blocking should be expanded to encompass cybersecurity-related blocking more generally, the better to structure the discretion carriers inevitably exercise in a threat-strewn traffic environment. But the framework adopted weakens the safeguards that make that approval legitimate and durable. It reduces both the information available to review system integrity, and the clarity of the limits governing its use. It lacks a structured and assessable reporting regime that secures legitimate confidentiality interests through meaningful oversight. And it narrows an existing privacy safeguard never put in issue by Compliance and Enforcement and Telecom Notice of Consultation 2025-143 (the Notice), which defined the boundaries of this proceeding and on which parties reasonably relied in deciding whether to intervene.

3. The written proceeding that produced the revised framework, conducted on a tight schedule between mid-June and late July 2025, drew participation from eight telecommunications service providers (TSPs)[1] and one law enforcement agency,[2] but no dedicated public-interest advocate, user group, or privacy intervener.[3] On that record, the majority has expanded a sensitive exception to a statutory prohibition without the benefit of adversarial testing, public-interest evidence, or privacy-focused scrutiny proportionate to the expansion.

---

[1] Bell Canada, Bragg Communications Inc. (doing business as Eastlink), Cogeco Communications Inc., Quebecor Media Inc., Rogers Communications Canada Inc., Saskatchewan Telecommunications, TekSavvy Solutions Inc., and TELUS Communications Inc. The Independent Telecommunications Providers Association registered as an intervener but provided no comments.

[2] The National Cybercrime Coordination Centre of the Royal Canadian Mounted Police.

[3] For instance, Compliance and Enforcement and Telecom Notice of Consultation 2021-9 drew interventions from the Privacy Commissioner of Canada; B.C. Civil Liberties Association; Canadian Association of the Deaf; Consumers' Association of Canada, National Anti-Poverty Organization, and Option consommateurs, represented jointly by the Public Interest Advocacy Centre; Canadian Internet Policy and Public Interest Clinic; Council of Canadians with Disabilities and ARCH Disability Law Centre; Open Internet Coalition; Participatory Culture Foundation; Union des consommateurs; and by creators' and labour guilds and unions and application and content providers, among others.

Telecommunications service providers as "trusted agents"

4. "Basic" telecommunications services offer a pure transmission capability over a communications path that is virtually transparent in terms of its interaction with information.[4] The Internet's shared numbering and routing protocols stitch together basic telecom links[5] that are not usable without measures to safeguard their pure transmission capability.[6] So TSPs necessarily exercise operational judgment in managing harmful or unwanted traffic. That puts TSPs in a sensitive role, described well by the Office of the Privacy Commissioner (OPC) as that of "trusted agents":

> Telecommunications service providers […] act as "trusted agents". They provide customers with access to Internet, mobile and landline phone services, and are in effect the pipeline through which all customers' mobile, telephone and internet communications, however sensitive, must flow. Customers entrust their private communications to their telecommunications service provider with the expectation that they will be delivered safely and securely, and that they will generally not be monitored unless it is for a purpose directly related to the provision of the service.[7]

5. Recognizing the sensitivity of this role, telecommunications regulation embeds common-carrier safeguards to structure the discretion TSPs may wield. In Canada these safeguards are anchored in two provisions of the Act: subsection 27(2), which prohibits unjust discrimination and undue preference; and section 36, which prohibits a carrier from controlling the content or influencing the meaning or purpose of telecommunications it carries for the public absent Commission approval.

6. In the centralized public switched telephone network, how to apply these safeguards was comparatively straightforward. Traffic management was to be "subject only to the technical parameters of fidelity or distortion criteria, or other conditioning." For instance, "techniques that facilitate economical, reliable movement of information [do] not alter the nature of the basic service." Similar for "internal speed, code and protocol conversion that is not manifested in the outputs of the service", and "service, memory or storage within the network".[8]

---

[4] Telecom Decision 84-18, subsection II.C.

[5] David D. Clark, *Designing an Internet* (Cambridge, MA: MIT Press, 2018).

[6] Craig McTaggart, "Was the Internet ever neutral?" Telecommunications Policy Research Conference, 15 August 2006.

[7] *Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program,* PIPEDA Report of Findings 2015-001 (Office of the Privacy Commissioner), 7 April 2015, citing Éloïse Gratton, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices* (Toronto: CCH Canada Ltd., 2003).

[8] Telecom Decision 84-18, subsection II.C.

7. How to apply common-carrier principles to the Internet, whose basic design is far less centralized, is correspondingly less settled.

Assessability and accountability

8. The Commission's 2009 framework for Internet traffic management required that TSPs shape such practices to address a defined need "and nothing else."[9] The Commission did not then venture deep into when Internet traffic might be blocked outright, section 36's domain, while remaining a basic telecommunications service.

9. With the full Commission's[10] majority decision above,[11] it now has. Carrier participation remains voluntary. But for subscribers of participating carriers, blocking applies by default. Technical workarounds such as Virtual Private Network services and alternative domain name resolvers are to be available to subscribers who seek them. But technical workarounds are not substitutes for accountability in how that discretion is exercised.

10. The framework for botnet blocking placed significant weight on transparency and reporting requirements. The revised framework for network-level blocking prefers greater reliance on carrier self-assessment and on confidential reporting, but without corresponding enhancements to public accountability. Where the earlier framework constrained authorization to indicator-based matching against authorized blocklists, the revised one authorizes any measure a carrier may deploy to block malicious traffic, constrained by general principles rather than defined mechanisms, and without processes to assess collateral damage, update and expiry mechanisms, or complaint handling with service standards. Nor is reliance on bottom-up complaints a salve: where blocking is automated, upstream-fed, or difficult for users to diagnose, erroneous blocking may not reliably generate complaints at all. The small enterprise whose Internet Protocol address inherits a poisoned reputation from a prior tenant, or whose lawful site shares hosting infrastructure with a malicious neighbour, experiences only that customers stop arriving. It has no

---

[9] Telecom Regulatory Policy 2009-657, paragraph 43, following a consultation prompted by a more specific 2008 complaint: see Telecom Decision 2008-108 and Telecom Public Notice 2008-19 (as modified).

[10] By "full Commission" I refer, as I have in past opinions, to a determination neither delegated to a subcommittee constituted by Commission by-law, nor assigned to a panel of Commissioners—not to any particular Commissioner's participation or non-participation in the determination. On subcommittees constituted by by-law, see paragraph 11(1)(b) and subsection 12(3) of the *Canadian Radio-television and Telecommunications Commission Act*, R.S.C., 1985, c. C-22. On the Chairperson's authority to establish panels by assigning cases, and members to cases, see *Shoan v. Canada (Attorney General)*, 2016 FCA 261, para 6.

[11] Following a process launched in 2021: Compliance and Enforcement and Telecom Notice of Consultation 2021-9; Compliance and Enforcement and Telecom Decision 2022-170; *Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety,* CRTC Interconnection Steering Committee Network Working Group Report NTRE080, 31 May 2023; Compliance and Enforcement and Telecom Decision 2025-142; Compliance and Enforcement and Telecom Notice of Consultation 2025-143.

reason to suspect carrier-level blocking, no notice that it occurred, and no third-party-overseen path to contest it.

11. A basic level of transparency helps users understand how their communications may be affected. It allows researchers, public interest groups, and other engaged parties to identify patterns and potential concerns. It lets subscribers take account of a provider's practices when making purchasing decisions. Competition cannot discipline what subscribers cannot assess. The revised framework significantly reduces disclosure requirements, both in terms of specificity and obligation, in ways that simplify disclosure but reduce observability. Disclosure that would expose defensive methods, thresholds, or specific configurations raises legitimate security concerns. Properly aggregated performance indicators, complaint pathways, and higher-level accountability safeguards do not.

12. As transparency decreases, so does the ability of competition, public scrutiny, and informed consumer choice to constrain carrier behaviour. Greater weight then falls on complaint handling and Commission oversight. A complaints process is still required, but is no longer meaningfully structured. The framework for botnet blocking treated complaints as quality-assurance and system-integrity inputs triggering review of the indicator at issue, correction where necessary, and communication back to the complainant. The revised framework recasts complaints as customer-service events rather than as structured inputs into system quality assurance. Left largely to carrier design disconnected from broader scrutiny, without classification, retention, or linkage to corrective action, such a framework cannot reliably surface or correct systemic error. Nor, therefore, can it perform the governance function on which the framework's principles-based authorization approach depends. If Commission oversight is most important where the Commission is the only actor with access to sensitive reporting data, then we have a distinct responsibility. It is to review the information we solely hold, identify system-level trends, and aggregate our findings for the public in a manner that protects confidentiality but promotes system integrity.

13. Carrier discretion is not self-legitimating. What renders it legitimate is a governance structure for visibility, review, and correction. An annual reporting requirement now captures only aggregate metrics without the contextual information needed to assess system quality. That is bookkeeping, not management. A carrier could report high blocking volumes and low complaint numbers while still operating with misconfigured rules, stale indicators, overbroad fingerprinting, or false positives that users did not detect or could not readily attribute to blocking. Without denominator, error-correction, and lifecycle information, reported volumes say little about accuracy or proportionality. Accountability requires information that can be assessed, not merely information that can be counted. Nor does the reporting framework require the Commission to aggregate confidential carrier reports into specific but consistent, year-on-year, public reporting. It provides only that the Commission "may" publish certain metrics or develop aggregated industry summaries. A framework of this kind should not depend on discretionary disclosure designed after the fact. Without information that connects outcomes to underlying processes, reporting cannot support meaningful third-party assessment.

14. A principles-based model can be made administrable without reverting to prescriptive technical rules. I would have required three things, each directed at making wrongful blocking findable by the affected subscriber, in the individual case, and by the Commission and public across the system.

15. First, structured annual reporting. Each participating carrier's annual report would include, at minimum,

    a) volume of traffic assessed relative to traffic blocked;

    b) basic lifecycle information (additions, retirements) for measures and third-party vendors in use;

    c) corrections made after having identified false positives; and

    d) complaint outcomes classified by disposition: blocking confirmed, modified, reversed, or not verifiable.

16. Reporting in this form connects outcomes to processes without disclosing defensive methods, thresholds, or configurations.

17. Second, restore to complaint processes their system integrity function. The botnet framework treated complaints as quality-assurance inputs. I would have carried that function forward by requiring blocking-related complaints to be acknowledged with minimum informational elements, logged, classified in a manner that permits audit and trend analysis, and subject to an escalation path that includes the Commission.

18. Third, Commission commitment, rather than Commission discretion. I would have committed us to regular publication of consistent, year-on-year, aggregated indicators that allow for market scrutiny, debate, and ecosystem benchmarking without compromising operational security.

19. Requirements like these for systemically important TSPs[12] would have structured accountability commensurate with the discretion conferred without prescribing technologies or methods, and in a manner that promotes good governance both internally and, under Commission oversight, sector-wide. To stop at whether information is being reported, confidentially by carriers to the Commission and by the Commission to the public, is to ask the wrong question. The right one is whether this information can at each step support assessment.

---

[12] TSPs whose overall size or position as a key provider in a region exceeds a given threshold, the former because their blocking determinations propagate widely, and the latter because their subscribers cannot easily route around them. On such thresholds and their relationship to minimum efficient scale (and therefore market entry and participation), see my remarks to the CanWISP Annual Conference, 31 March 2026.

Privacy safeguards

20. The Commission is not a general privacy regulator. But it has sector-specific responsibilities requiring expressly that it contribute to the protection of privacy.[13] A general privacy principle holds that personal information "shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law."[14] Consistent with these responsibilities and with that privacy principle, the framework to limit botnet traffic did "not permit any additional collection, use, or disclosure of personal information."[15]

21. The Notice initiating this proceeding[16] posed five questions (of 12) relating to privacy. Two collected factual information. The other three, entitled "Addition of safeguards to the framework to help protect privacy," asked whether further privacy safeguards were required in addition to those already in place. The revised framework's treatment of privacy goes wrong in three distinct ways. First, it adds no safeguards, notwithstanding a material expansion in the sensitivity and granularity of the techniques it authorizes. Second, the one new limit it does impose on deep packet inspection is not administrable as written. Third, it narrows an existing safeguard that the Notice never put in issue.

22. First, an important distinction should be kept in view. The previous framework, limited largely to blocklist-based blocking, sat at the lower end of the intrusiveness spectrum. The expansion to techniques like file signatures, traffic anomaly detection, and network fingerprinting is materially different. Static matching against indicators of compromise like Internet Protocol addresses, Autonomous System numbers, host names, or similar identifiers asks whether traffic corresponds to an identified string. The behavioural analysis needed to support some of the newly-admitted techniques requires more sustained traffic observation at a level of granularity that is content-proximate, if not content-revealing, whether in building a baseline model of what "normal" traffic looks like for traffic anomaly detection, or identifying traffic flow characteristics like timing, volume, protocol patterns, or payload signatures for network fingerprinting. Even where they do not inspect content as such, these techniques can generate or support inferences about identifiable accounts, endpoints, or patterns of use. The privacy implications are different in kind, not only in degree.

23. Where the scope of authorized measures grows to include techniques that are more observational, inferential, or persistent, the corresponding governance structure must grow in tandem. A finding

---

[13] Act, paragraphs 7(i) and 47(a).

[14] *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5), Schedule 1, clause 4.5.

[15] Compliance and Enforcement and Telecom Decision 2025-142, Appendix, subsection 8.2.

[16] Compliance and Enforcement and Telecom Notice of Consultation 2025-143, paragraph 4, Q6 through Q10.

that no additional safeguards are required sits uneasily with material expansion in the sensitivity and granularity of the information collected. Notwithstanding that material expansion, the majority finds that no additional privacy safeguards are needed beyond those already established, then immediately singles out deep packet inspection (DPI) for special limitation. That juxtaposition highlights the problem. If one of the newly contemplated techniques requires express rules because of its privacy implications, the premise that no additional safeguards are needed becomes difficult to sustain. The majority does not explain why existing safeguards were sufficient in view of the broader range of techniques and more sensitive forms of information at play. The framework should have set out how TSPs are expected to steward and report on these techniques.

24. Second, the majority recognizes that DPI raises distinct privacy concerns, and therefore states that its use must be limited to "exceptional circumstances." This is necessary, but the framework does not make the rule administrable. It does not define what qualifies as exceptional; how long such a use may continue post-breach; what records must be created; or how the Commission is to review consistency across carriers, or the public to be assured of it.

25. A workable safeguard would, at minimum, require that the exceptional circumstances be specifically justified, time-limited, documented, attributable to a designated decision-maker, and reviewable after the fact. The framework does none of those things. Nor does it explain whether the examples given (court orders and post-incident tuning) are exhaustive or merely illustrative, whether affected users may complain specifically about such use, or how this rule relates to the Commission's existing framework for Internet traffic management practices. Without such elements, the rule is not readily auditable or consistently applicable across carriers.

26. Third, where the botnet framework prohibited the reuse of already-collected personal information for other purposes, like behavioural advertising, the revised framework relaxes that protection by providing that no additional collection, use, or disclosure of personal information is permitted "except where such activities are authorized by applicable laws and regulations or by an order from a court of competent jurisdiction." That opens the door to secondary uses that the earlier framework foreclosed.

27. Traffic observation justified by security may yield profiles valuable for marketing. The revised wording leaves carriers to judge for themselves how far the one may feed the other. That change is both substantively troubling and procedurally unsupported. It weakens a purpose-limitation safeguard just as the framework expands to techniques capable of generating more sensitive traffic-related information. It does so even though the Notice asked whether additional safeguards should be added, not whether existing safeguards should be narrowed, framing the live issue as whether protection should grow. Potential interveners calibrate their participation to the questions asked; a relaxation the Notice did not signal is not one the record was to test.[17] I would have

---

[17] *Bell Canada v. Canada (Attorney General)*, 2016 FCA 217, paragraph 38, *a contrario* (notice of consultation provided fair notice that the entire practice of simultaneous substitution was up for discussion; the converse condition obtains

retained the existing purpose-limitation language and, had the Commission considered relaxation worth exploring, put that proposal to a record built for purpose.

28. Trusted agents should not be left to infer, from silence, how far they may repurpose information obtained in the course of securing communications. The majority acknowledges that the OPC has in place a policy framework for online behavioural advertising. That framework, issued in another context but not long after the OPC identified telcos as trusted agents whose customers expect "that they will generally not be monitored unless it is for a purpose directly related to the provision of the service,"[18] cautions that online behavioural advertising "should not be considered a term or condition for individuals to use the Internet generally."[19] It requires that users both be made aware of the proposed use in a manner that is clear and understandable, and first be able easily to opt out in a way that takes effect immediately and persistently.

29. These requirements relate to consumer notification and consent. They attach before any de-identification or aggregation of traffic data:[20] consent is not to be bootstrapped after the fact by stripping identifiers from personal information that ought not have been repurposed at all. Carriers wishing to pursue secondary uses, and interveners wishing to contest them, will find the natural venue in the consumer-facing terms on which telecommunications services are contracted.

Conclusion

30. The majority authorizes a broader range of cybersecurity techniques operating on a larger and more sensitive set of traffic-related information, in a framework that functions as on by default, yet remains barely visible to those subject to it. The expansion itself is needed. Weakening the safeguards that structure it is not. As carrier discretion expands, the transparency, accountability, and privacy protections governing that discretion should expand in step. Instead, the revised framework inverts the relationship. "Trusted agent" is not a status carriers hold. It is a standard to which they must be held. I respectfully dissent.

---

here). See also my dissent in Telecom Notice of Consultation 2024-293 (as a result of the style of notice of consultation, "end-of-discount and end-of-contract updates to the Television Service Provider Code similar to those contemplated for the Wireless Code and the Internet Code will not be possible on this proceeding").

[18] PIPEDA Report of Findings 2015-001, cited at footnote 7 in this dissenting opinion.

[19] *Office of the Privacy Commissioner of Canada* (2015), Policy position on online behavioural advertising.

[20] See majority decision, above, at its footnote 9.

Related documents

- *Call for comments – Proposed modifications to the framework to limit botnet traffic*, Compliance and Enforcement and Telecom Notice of Consultation CRTC 2025-143, 13 June 2025

- *Development of a framework to limit botnet traffic*, Compliance and Enforcement and Telecom Decision CRTC 2025-142, 13 June 2025

- *Call for comments – Making it easier to choose a wireless phone or Internet service – Enhancing customer notification,* Telecom Notice of Consultation CRTC 2024-293, 22 November 2024, as amended by Telecom Notices of Consultation CRTC 2024-293-1, 20 December 2024; 2024-293-2, 14 February 2025; and 2024-293-3, 28 February 2025

- *Public Interest Advocacy Centre – Request to define the privacy requirements for telecommunications service providers in the context of any digital contact tracing technologies app*, Telecom Decision CRTC 2022-238, 6 September 2022

- *Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety*, Compliance and Enforcement and Telecom Decision CRTC 2022-170, 23 June 2022, as amended by Compliance and Enforcement and Telecom Decision CRTC 2022-170-1, 11 October 2022

- *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, as amended by Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9-1, 29 June 2021

- *Application of regulatory obligations directly to non-carriers offering and providing telecommunications services*, Telecom Regulatory Policy CRTC 2017-11, 17 January 2017, as amended by Telecom Regulatory Policies CRTC 2017-11-1, 10 July 2017, and 2017-11-2, 17 July 2018

- *Regulatory measures associated with confidentiality provisions and privacy services*, Telecom Regulatory Policy CRTC 2009-723, 25 November 2009

- *Review of the Internet traffic management practices of Internet service providers,* Telecom Regulatory Policy CRTC 2009-657, 21 October 2009

- *Accessibility of telecommunications and broadcasting services*, Broadcasting and Telecom Regulatory Policy CRTC 2009-430, 21 July 2009, as amended by Broadcasting and Telecom Regulatory Policy CRTC 2009-430-1, 17 December 2009

- *The Canadian Association of Internet Providers' application regarding Bell Canada's traffic*

shaping of its wholesale Gateway Access Service, Telecom Decision CRTC 2008-108, 20 November 2008

- *Review of the Internet traffic management practices of Internet service providers,* Telecom Public Notice CRTC 2008-19, 20 November 2008, as amended by Telecom Public Notices CRTC 2008-19-1, 11 February 2009; 2008-19-2, 12 February 2009; 2008-19-3, 18 March 2009; and 2008-19-4, 16 July 2009

- *Confidentiality provisions of Canadian carriers*, Telecom Decision CRTC 2003-33, 30 May 2003, as amended by Telecom Decision CRTC 2003-33-1, 11 July 2003

- *Enhanced Services,* Telecom Decision CRTC 84-18, 12 July 1984