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

# Compliance and Enforcement and Telecom Notice of Consultation CRTC 2025-143

PDF version

Gatineau, 13 June 2025

*Public record: 1011-NOC2025-0143*

## Call for comments – Proposed modifications to the framework to limit botnet traffic

**Deadline for submission of interventions: 14 July 2025**

**Deadline for submission of replies: 29 July 2025**

[Submit an intervention or view related documents]

### 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 regulating telecommunications service providers (TSPs). 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. In Compliance and Enforcement and Telecom Decision 2022-170, the Commission found that regulatory action is necessary so that TSPs can help disrupt botnets and protect Canadians from the harm they cause. The Commission also outlined the guiding principles for a regulatory framework to block harmful botnet activities in that decision.

In Compliance and Enforcement and Telecom Decision 2025-142, the Commission established a framework that sets out the terms and conditions to allow Canadian carriers to block botnets and other harmful activities within their networks before reaching Canadians' devices. Currently, the framework only allows the use of blocklists.

In this notice, the Commission is gathering views on whether the framework should be expanded to include other blocking methods.

Canada

## Background

1. In Compliance and Enforcement and Telecom Decision 2025-142, the Commission established a framework that sets out the terms and conditions allowing Canadian carriers to block botnets and other harmful activities at the network level before reaching Canadians' devices. Currently, the framework only allows the use of blocklists. Blocklists are lists of information that help identify harmful activity. Carriers can use these lists to block suspicious or dangerous online traffic from passing through their networks.

2. The Commission is considering expanding the scope of the final framework to include other blocking methods, such as those based on file signatures, traffic volume anomalies, and network fingerprinting. Since the Commission currently has limited information about these other blocking methods, it is initiating this public consultation to gather comments on whether, and how, they should be incorporated into the framework and, if so, whether additional privacy safeguards and reporting requirements are needed.

## Call for comments

3. The Commission welcomes submissions on the questions below. Interested persons are invited to answer those questions that are of interest to them and are not required to answer all questions. Definitions and reports that may help parties prepare their responses are listed in the appendix to this notice.

### Canadian carriers' current use of, or intention to use in the future, blocking methods that are different from what is described in section 2 of the framework

4. The Commission is gathering information on how Canadian carriers' blocking methods work. Views from all parties on these methods are welcome. This information will help the Commission determine if more methods should be allowed and, if so, under what conditions.

Q1. Do you currently use, or plan on using, port blocking? If so, which particular port(s)/protocol(s) are being, or would be, blocked?

Q2. Do you currently block, or plan on blocking, Internet traffic that includes a forged source address? If so, what procedures are being, or would be, used to determine that a source Internet Protocol (IP) address has been forged?

Q3. Do you currently block, or plan on blocking, Internet traffic based on file signatures?

(i) If so, what indicator(s) are being, or would be, used to detect and block Internet traffic with this method (e.g., cryptographic hashes of malicious binaries or scripts, or code signing certificates in binaries)?

(ii) Where do these indicators come from (e.g., in-house or third-party blocklists)?

(iii) Should this blocking method be incorporated into a blocklist and, if so, are adjustments to the framework required (e.g., the definition of indicator of compromise or the requirements applicable to the use of blocklists)?

Q4. Do you currently block, or plan on blocking, Internet traffic based on traffic volume anomalies to prevent volumetric attacks?

Q5. Do you currently use, or plan on using, any other network-level blocking methods not identified in the previous questions (e.g., methods based on network fingerprinting)? If so, describe each of these other methods.

**Privacy issues related to all blocking methods**

Q6. When monitoring data point(s) for network-level blocking, are deep packet inspection (DPI) or other similar techniques used?

(i) If so, are only packet headers inspected, or is the content of communications also inspected (when unencrypted)?

(ii) What data point(s) are inspected using DPI for detecting and blocking malicious Internet traffic?

Q7. For any detection and blocking methods, is personal information collected, logged, or retained on network control points or otherwise?

(i) If so, what is the retention period and who has access to the personal information?

(ii) How is this personal information used and disclosed?

(iii) If this personal information is aggregated and anonymized, how is it used and disclosed?

**Addition of safeguards to the framework to help protect privacy**

Q8. When using blocking methods other than blocklists, should carriers be prohibited from examining, analyzing, or keeping the contents of electronic communications? If so, why?

Q9. Should carriers be prohibited from using or disclosing any of the information collected under the framework (e.g., a household's traffic volume or visited websites) for any other purposes (e.g., targeted advertising)? If so, why?

Q10. Should carriers be prohibited from keeping packet header information, or from keeping such information beyond an acceptable amount of time? If so, why?

### Addition of reporting obligations to the framework if additional blocking methods are allowed

Q11. If the Commission decides to allow any of the blocking methods listed in Q1–Q5, should it adjust the reporting requirements of the framework to improve transparency of carriers' blocking performance (e.g., statistics on signature-based blocking)?

Q12. Keeping in mind that the Commission wants the framework to be technologically neutral and flexible, should carriers be asked to report their blocking methods every year? If not, explain why.

## What you need to know to participate in this proceeding

### Procedure

5. The *Canadian Radio-television and Telecommunications Commission Rules of Practice and Procedure* (the Rules of Procedure) apply to this proceeding. The Guidelines on the CRTC Rules of Practice and Procedure (Broadcasting and Telecom Information Bulletin 2010-959) are meant to help members of the public understand the Rules of Procedure so that they can more effectively participate in Commission proceedings.

6. The Commission encourages responses from, among others, incumbent and competitive local exchange carriers, vendors, protective Domain Name System (DNS) providers, web hosting companies, and governmental organizations whose mandates include safeguarding critical infrastructure, computer networks, or personal information.

### Submitting interventions and replies

7. The Commission invites comments that address the issues and questions set out above. The Commission will accept interventions that it receives no later than **14 July 2025**.

8. Interested persons who require assistance submitting comments can contact the Commission's Hearings & Public Proceedings group at hearing@crtc.gc.ca.

9. Interested persons who file an intervention automatically become a party to this proceeding. Only parties to the proceeding can participate in further stages of the proceeding. The deadline for filing replies is **29 July 2025**. Replies may address any matters on the record of the proceeding.

10. Submissions must be filed by sending them to the Secretary General of the Commission using only one of the following means:

    - completing the Commission's intervention form;
    - sending a fax to the Commission at 819-994-0218; or

- writing to the Commission by mail to CRTC, Gatineau, Quebec K1A 0N2.

11. Submissions longer than five pages should include a summary. Submissions will be posted in the official language and format in which they are received.

12. The deadline to submit an intervention to the Commission is 5 p.m. Vancouver time (8 p.m. Gatineau time). Parties are responsible for ensuring the timely delivery of their submissions and will not be notified if their submissions are received after the deadline. Late submissions will not be considered by the Commission and will not be made part of the public record.

### Privacy notice

13. Please note the following:

    - Documents will be posted on the Commission's website exactly as received. This includes any personal information contained in them, such as full names, email addresses, postal/street addresses, and telephone and fax numbers.

    - All personal information parties provide as part of this public process, except information designated as confidential, will be posted on the Commission's website and can be accessed by others.

    - However, the information parties provide can only be accessed from the web page of this particular public proceeding. As a result, a general search of the Commission's website using either its search engine or a third-party search engine will not provide access to the information that was provided as part of this public proceeding.

    - The personal information that parties provide will be used and may be disclosed for the purpose for which the information was obtained or compiled by the Commission or for a use consistent with that purpose.

### Confidentiality

14. The Commission's proceedings are designed to allow members of the public to provide input so that it can make better, more informed decisions. As a result, the general rule is that all information filed with the Commission is placed on the public record and can be reviewed by all parties and members of the public.

15. However, the Commission also often needs detailed information from the companies it regulates and supervises to make an informed decision. This information can be commercially sensitive, especially as the environment in which the companies operate becomes more competitive. The Commission will therefore accept certain information as confidential.

16. Parties can request that information be filed in confidence under subsection 39(1) of the *Telecommunications Act* with a detailed rationale as to why that information

should be considered confidential. The Commission reminds parties that make such a request that when a document is filed with confidential information, an abridged version must also be filed so that it can be included in the public record.

### Accessible formats for people with disabilities

17. The Commission requires regulated entities and encourages all parties to file submissions in accessible formats (e.g., text-based file formats that enable text to be enlarged or modified or read by screen readers) for this proceeding. To help in this regard, the Commission has posted on its website guidelines for preparing documents in accessible formats.

18. If submitted documents have not been filed in accessible formats, you can contact the Commission's Hearings & Public Proceedings group at hearing@crtc.gc.ca to request that Commission staff obtain those documents in accessible formats from the party that originally submitted the documents in question.

### Accessing documents

19. Links to interventions, as well as other documents referred to in this notice, are available on the Commission's "Consultations and hearings: have your say" page.

20. Documents are available upon request during normal business hours by contacting:

    Documentation Centre
    Examinationroom@crtc.gc.ca
    Tel.: 819-997-4389
    Fax: 819-994-0218

    Client Services
    Toll-free telephone: 1-877-249-2782
    Toll-free TTY: 1-877-909-2782

21. Interested persons can find electronic versions of the documents by clicking on "[Submit an intervention or view related documents]" at the top of this notice.

Secretary General

## Related documents

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

- *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

- *Guidelines on the CRTC Rules of Practice and Procedure*, Broadcasting and Telecom Information Bulletin CRTC 2010-959, 23 December 2010

# Appendix to Compliance and Enforcement and Telecom Notice of Consultation CRTC 2025-142

## Port blocking

See Port Blocking, Broadband Internet Technical Advisory Group, August 2013.

Blocking SMTP [Simple Mail Transfer Protocol] traffic on port 25, for example, is a common practice to prevent spam, as recommended in the following reports:

- Managing Port 25 for Residential or Dynamic IP Space – Benefits of Adoption and Risks of Inaction, Messaging Anti-Abuse Working Group, 2005

- Recommended Internet Service Provider Security Services and Procedures, Request for Comments (RFC) 3013, Tom Killalea, Internet Engineering Task Force (IETF), November 2000 (RFC 3013)

The following also note that carriers effectively use this practice:

- Paragraphs 52–53 of *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

- ISP's anti-spam measures questioned, PIPEDA Case Summary #2005-319, Office of the Privacy Commissioner of Canada (OPC), 8 November 2005

## Forged source address

Refer to the following reports:

- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, Paul Ferguson and Daniel Senie, The Internet Society, May 2000 (RFC 2827)

- Ingress Filtering for Multihomed Networks, RFC 3704, Fred Baker and Pekka Savola, The Internet Society, March 2004 (update to RFC 2827)

- RFC 3013

- Security Best Practices for Canadian Telecommunications Service Providers (TSPs) [section 3.1.4, control 2], Canadian Security Telecommunications Advisory Committee (CSTAC), 31 October 2013

### Blocking Internet traffic based on file signatures

This method relies on recognizing known patterns of malware distribution, execution, or other behaviours that characterize system infections or known attack methods. Real-time traffic is compared against a repository of signatures and blocked in the event of a match.

Network Security and Monitoring Detection Standard for Canadian Telecommunications Service Providers (CTSPs), Canadian Telecommunications Cyber Protection working group for CSTAC, 20 January 2020, states that TSPs should have the capability to detect malware operating within their networks by signature. Furthermore, responses to Commission requests for information show that Rogers Communications Canada Inc., Shaw Communications Inc., TekSavvy Solutions Inc., and Xplornet Communications Inc. each use some form of signature-based blocking as part of their respective blocking strategies.

### Blocking information based on network fingerprinting

A grouping of information based on the exchange that occurs between two devices when initiating a connection over the Internet (i.e., based on information exchanged in a TCP [Transmission Control Protocol] three-way handshake). Elements of this exchange that can categorize the purpose of a device, even malicious devices, include the number of times a device attempts to retransmit or the time between retransmissions. When unique enough, these elements can be used to fingerprint command and control servers and other malicious devices.

### Deep packet inspection

Deep packet inspection (DPI) is a form of computer network packet filtering that has been available for several years. When used for a cyber security purpose, DPI may examine the data or header portions of a packet as it passes an inspection point, searching for indications of protocol non-compliance, malware, and other forms of intrusion.

DPI technologies raise privacy concerns because they can involve the inspection of information sent over the Internet, as indicated in the OPC's submission and final reply to the Commission in the context of the Internet traffic management practices proceeding that led to *Review of the Internet traffic management practices of Internet service providers*, Telecom Regulatory Policy CRTC 2009-657, 21 October 2009.

Open Xchange and Vaxination Informatique initially advised against authorizing DPI, while TELUS Communications Inc. mentioned in its contribution to the CRTC Interconnection Steering Committee that botnet blocking at other layers such as DPI is useful and should be encouraged, thus suggesting that it is already in use.

In Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection, PIPEDA Report of Findings #2009-010, September 2009, the OPC recommended that Bell Canada inform its customers about DPI it was performing. However, it is unclear whether this recommendation has been implemented by Bell Canada and other carriers using the same technology.