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

Compliance and Enforcement and Telecom Regulatory Policy CRTC 2016-442

PDF version

Reference: Compliance and Enforcement Notice of Consultation 2015-333, as amended

Ottawa, 7 November 2016

File number: 8665-C12-201507576

Empowering Canadians to protect themselves from unwanted unsolicited and illegitimate telecommunications

The Commission finds that the technical solutions available to Canadians to protect themselves from unwanted unsolicited and illegitimate telecommunications are not sufficient. As such, the Commission sets out its findings on technical solutions that Canadians could use to protect themselves from unwanted unsolicited and illegitimate telecommunications and, for the purposes of empowering and informing Canadians, ***directs*** *telecommunications service providers that provide retail voice services to report to the Commission,* ***within 180 days*** *of the date of this decision, details on the opt-in filtering service(s) they offer or propose to offer to their subscribers.*

In addition, to ensure that all Canadians benefit from a base level of protection from nuisance calls, the Commission requests the CRTC Interconnection Steering Committee (CISC) to develop practices to block blatantly illegitimate calls at the network level. CISC is to provide a report of its findings to the Commission ***within 90 days*** *of the date of this decision. Blatantly illegitimate calls include calls that purport to originate from telephone numbers that (i) match the telephone number of the person being called; (ii) are "spoofed" with a number that is local to the person being called, in the case of an incoming long distance call; or (iii) do not conform to the North American Numbering Plan (i.e. are non-dialable telephone numbers [e.g. 000-000-0000]).*

The Commission is prepared to take further action if it becomes clear that the industry is not taking sufficient measures to protect Canadians against unwanted calls.

Given the complexities associated with caller identification (caller ID) "spoofing," and the rapid evolution of work done since the closing of the record of this proceeding, the Commission intends to launch a follow-up process to review the progress being made on the issue of caller ID authentication.

Introduction

1. The Commission regulates unsolicited telecommunications pursuant to sections 41 to 41.7 and 72.01 to 72.15 of the *Telecommunications Act* (the Act). Subsection 41(1) specifies that

> The Commission may, by order, 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.

2. The Commission, in Telecom Decision 2007-48, established the Unsolicited Telecommunications Rules (UTRs),[1] which is a comprehensive framework for the regulation of unsolicited telecommunications. The UTRs include the National Do Not Call List (DNCL) Rules, the Telemarketing Rules, and the Automatic Dialing-Announcing Device (ADAD)[2] Rules. The UTRs and the National DNCL came into operation on 30 September 2008.

3. It is becoming increasingly difficult for agencies worldwide, including the Commission, to stop unwanted unsolicited and illegitimate telecommunications (nuisance calls[3]) when callers are using the practice of caller identification (caller ID)[4] "spoofing."[5] This practice, which can accentuate the harm caused by nuisance calls, occurs when callers conceal or misrepresent their true identity by displaying fictitious phone numbers when making calls. Caller ID spoofing may also be used to facilitate misleading and fraudulent telemarketing activities, which may lead to anxiety, annoyance, and, in some cases, distress and financial losses. Based on its own analysis, the Commission estimates that 45% of the complaints received by the National DNCL Operator in 2015 involved an element of illegitimate caller ID spoofing.

4. Given the important role that telecommunications play in the lives of all Canadians, the Commission strives to ensure that all Canadians have adequate protection when accessing the communication system. To do so, the Commission recognizes that the collaboration of a number of stakeholders, including individual Canadians, is vital to properly examine, develop, and implement technical solutions that could provide ubiquitous protection to Canadians regardless of the platform they use (i.e. traditional wireline, wireless, or voice over Internet Protocol [VoIP]).

---

[1] For further details on the UTRs, see the Commission's web page on Understanding telemarketing rules for compliance.

[2] "ADAD" refers to any automatic equipment incorporating the capability of storing or producing telecommunications numbers, used alone or in conjunction with other equipment, to convey a pre-recorded or synthesized voice message to a telecommunications number. Calls made by ADADs are sometimes referred to as "robocalls."

[3] For the purpose of this proceeding, the term "nuisance calls" refers to unwanted unsolicited and illegitimate telecommunications made for the purpose of selling or promoting a product or service or for the solicitation of money or money's worth (i.e. telemarketing telecommunications), or for other purposes (e.g. market research, surveys, or public opinion polls, or calls to collect overdue accounts). Unsolicited calls are not necessarily illegitimate under the UTRs.

[4] Caller ID displays the calling party's telephone number and/or name on devices supported by the network.

[5] A spoofed number can appear as a string of digits, such as 000-000-0000, a random number, or the number of a company, person, or government entity. Telemarketers who make sales calls to consumers in Canada have an obligation to identify themselves. Callers who use technology to spoof their caller ID information with inaccurate, false, or misleading information violate this requirement. Spoofed calls are not necessarily illegitimate under the UTRs.

5. Accordingly, in Compliance and Enforcement Notice of Consultation 2015-333, the Commission initiated a proceeding to

   - gather information regarding available technical solutions that Canadians may leverage to protect themselves from nuisance calls;

   - solicit comments on the use, effectiveness, and limitations of available solutions, particularly in relation to more vulnerable groups of Canadians; and

   - identify any barriers, including legal or regulatory prohibitions, to the adoption of existing solutions or to the implementation of new and innovative solutions (e.g. call blocking, user reporting).

6. The Commission received interventions from the following: the Public Interest Advocacy Centre (PIAC); numerous individuals; Bell Canada,[6] MTS Inc. and Allstream Inc. (collectively, MTS Allstream), Saskatchewan Telecommunications (SaskTel), and TELUS Communications Company (TCC) [collectively, the incumbent local exchange carriers, or ILECs]; Bragg Communications Incorporated, operating as Eastlink (Eastlink); the Canadian Independent Telephone Company Joint Task Force, on behalf of the members listed in the Appendix to this decision (JTF); the Canadian Network Operators Consortium Inc. (CNOC); Cido Research Inc.; Cogeco Cable Inc., on behalf of Cogeco Cable Canada LP and Cogeco Cable Québec General Partnership; Distributel Communications Limited; Fibernetics Corporation; Google Inc. (Google); Ice Wireless Inc.; InnSys Voice Corp.; Iristel Inc.; Kedlin Company Inc. (Kedlin); Managed Network Systems, Inc.; Microsoft Corporation (Microsoft); Mustel Group; Novus Entertainment Inc. (Novus); Primus Telecommunications Canada Inc. (Primus); Quebecor Media Inc., on behalf of Videotron G.P. (Videotron); Rogers Communications Partnership (RCP);[7] Shaw Communications Inc. (Shaw); TBayTel; TekSavvy Solutions Inc.; Telephone Science Corporation (TSC); trueCall Limited (trueCall); and WIND Mobile Corp.

7. To assist Canadians in formulating their comments for this proceeding, the Commission, on 20 November 2015, published on its website a summary list of features and options that were identified by telecommunications service providers (TSPs) as being currently available in the Canadian market to help Canadians protect themselves from nuisance calls. On the same day, the Commission issued a news release encouraging the industry to pay special attention to the comments being submitted in this proceeding by their customers who want help to reduce illegitimate caller ID spoofing.

---

[6] Bell Canada intervened on behalf of itself and Bell Aliant Regional Communications, Limited Partnership; Bell Mobility Inc.; DMTS; KMTS; NorthernTel, Limited Partnership; Northwestel Inc.; O.N. Tel Inc., operating as Ontera; and Télébec, Limited Partnership.

[7] RCP ceased to exist as of 1 January 2016. All of its business activities, including its assets and liabilities, are now held by Rogers Communications Canada Inc.

8. The public record of this proceeding, which closed on 31 January 2016, is available on the Commission's website at www.crtc.gc.ca or by using the file number provided above.

Issues

9. The Commission has identified the following issues to be addressed at this time:

    - Do Canadians have access to sufficient and effective call-management options to protect themselves against nuisance calls?
    - What solutions could TSPs introduce to better protect Canadians from nuisance calls?
    - What regulatory issues need to be addressed?

10. The Commission's analysis and determinations set out in this decision relating to these issues address a number of problems associated with caller ID spoofing. However, the Commission considers that the matter of caller ID spoofing warrants further examination such that technical standards can be developed and deployed by as many carriers in Canada.

11. In this regard, the Commission notes that, subsequent to the close of record of this proceeding, the Alliance for Telecommunications Industry Solutions (ATIS)[8] issued a report in April 2016 titled *Calling Party Spoofing Mechanisms and Mitigation Techniques*. In that report, ATIS indicated that "the end goal is to give consumers the tools to reduce unwanted and fraudulent calls [and that] mitigating illegitimate Caller ID spoofing will not by itself fully achieve this goal." ATIS further indicated that a layered approach, similar to that used in cybersecurity efforts, with a range of choices of mitigation techniques, provides the flexibility to respond to an evolving threat.

12. Given the rapid evolution of work done in this area since the close of the record of this proceeding, the Commission intends to launch a follow-up process to review the progress being made by standards bodies on the issue of caller ID authentication. The areas to be considered include assessing the scope and limitations of standards being developed by those bodies, and ascertaining the implications for their implementation in Canada, in order to implement solutions that help ensure that Canadians' privacy is protected.

Do Canadians have access to sufficient and effective call-management options to protect themselves against nuisance calls?

13. A large proportion of the over 260 individual Canadians who intervened in this proceeding submitted that the current technical solutions are neither sufficient nor effective, indicated frustration with continuing to receive nuisance calls, and requested easy ways to block nuisance calls, including those that make use of ADADs.

---

[8] The main industry bodies involved in the creation of caller ID authentication standards are ATIS, a North American carrier group, and the Internet Engineering Task Force.

14. Eastlink and MTS Allstream submitted that basic calling features, such as call display and voice mail,[9] enable Canadians to recognize and manage nuisance calls by avoiding calls from unfamiliar callers.

15. Other TSPs submitted that existing calling features provide subscribers with some protection against nuisance calls, but recognized that caller ID spoofing limits their effectiveness. For its part, RCP submitted that existing calling features were not designed to combat nuisance calls.

16. A number of parties submitted that call-rejection solutions that rely on a personal blacklist[10] offer protection to consumers, but acknowledged that this feature provides no method for identifying nuisance calls that can originate from countless sources, of which consumers have no advance knowledge. Given that consumers often must actively and manually add nuisance numbers to their personal blacklist, they can generally only effectively protect themselves from the numbers appearing on their customized list. Some parties also referred to other selective call-rejection solutions, which can be used to block, for example, calls from certain area codes, international numbers, or private/unknown (anonymous) numbers. Bell Canada and TCC offer enhanced anonymous-call-management features that do not reject or block all anonymous calls. Rather, anonymous callers are prompted to enter a telephone number that will be displayed to the intended recipient. This approach generally prevents the subscriber from receiving robocalls from anonymous callers, because the robocall cannot typically respond to the prompt.

17. RCP and TCC submitted that call-acceptance solutions that rely on a personal whitelist[11] require the consumer to enter all numbers from which they wish to receive calls, which, according to TCC, is an onerous and unsustainable process that leaves the customer at risk of missing urgent and important calls.

18. Some parties indicated that their subscribers can flag nuisance calls using the pay-per-use Call Trace feature by dialing a code on their phone, which records information regarding their last call for review by the appropriate law enforcement agencies. However, Bell Canada and SaskTel stated that this feature is intended for harassing and threatening calls rather than nuisance calls.

19. Parties also indicated that Canadians could use devices that are specifically designed to manage nuisance calls for landlines.

---

[9] Voice mail enables the subscriber to use a system in which callers can leave a recorded message to be retrieved at the subscriber's convenience.

[10] Blacklists enable the subscriber to block certain calls based on caller ID information. The user manually selects the list of telephone numbers to block; it is generally limited to 10 to 30 telephone numbers per list.

[11] Whitelists enable the subscriber to accept certain calls based on caller ID information. The user manually selects the list of telephone numbers to accept; it is generally limited to 10 to 30 telephone numbers per list.

- Videotron referred to trueCall and CPR[12] Call Blocker, but did not provide any detailed observations regarding their availability, use, or effectiveness.

- trueCall indicated that its technology is able to manage nuisance calls, including those that are made using caller ID spoofing, and is integrated into a number of widely distributed cordless telephones in the United Kingdom.

20. A number of interveners also submitted that wireless subscribers could rely on applications built into the operating systems of their smartphones, or other applications developed by third parties, to block nuisance calls.

    - Microsoft and Google indicated that their wireless devices offer a feature that blocks all calls during certain hours, except calls from numbers specified by the user.
    - Kedlin noted that it provides an application for use on Android-based and Blackberry smartphones that is capable of identifying and blocking nuisance calls, including those that use caller ID spoofing, based on data that is aggregated in real time using a proprietary algorithm.

21. SaskTel suggested that it might be appropriate to offer free number reassignments to consumers who receive an excessive number of nuisance calls.

22. PIAC argued that current call-blocking options do not offer a complete solution, particularly considering how quickly telemarketers using illegitimate means change phone numbers. Further, PIAC indicated that while some of the applications may be an effective remedy to the problem of nuisance calls, not all consumers have the necessary technical equipment (such as a smartphone) or are able to afford the cost to subscribe to certain calling features.

Commission's analysis and determinations

Basic calling features

23. Some Canadians may receive more nuisance calls than others, and may be more vulnerable than others to distress and financials losses resulting from misleading or fraudulent telemarketing calls.

24. Accordingly, the Commission considers that Canadians require protection from nuisance calls that reflects their distinct circumstances, and that no one calling feature can possibly respond to the needs of all Canadians.

25. While recognizing that there are several basic calling features available to Canadians to help them manage certain types of nuisance calls, the Commission considers that they either

---

[12] CPR stands for Call Prevention Registry.

- require manual intervention from the consumer;
- rely solely on the individual consumer's ability to distinguish nuisance calls from other calls based solely on caller ID information;
- do not, in the case of call display and voice mail, prevent the inconvenience or nuisance of receiving the nuisance call; or
- may lead to blocking legitimate and wanted calls.

Smartphone applications

26. While there may be many smartphone applications available to Canadians to help manage certain types of nuisance calls, very limited information and comments were placed on the record of this proceeding regarding their use by Canadians and their effectiveness at identifying and managing nuisance calls.

27. As is the case for basic calling features, there are a number of limitations to the effectiveness of smartphone applications. Most require manual intervention from the user (i.e. they must be installed and configured); they limit the number of calls that they block or allow; and they may lead to unintended consequences such as blocking of wanted or legitimate calls. Furthermore, these applications are only available for smartphones, thus wireline and non-smartphone users cannot benefit from them.

End-user devices

28. Landline subscribers in the United Kingdom have access to several devices offering a variety of call-blocking capabilities. These include various handsets, as well as purpose-built devices that can be used with any landline handset. However, none of these products are sold in Canada, and the record of this proceeding did not disclose evidence of comparable products that are made available to Canadians.

Phone number reassignment

29. With regard to SaskTel's suggestion to offer free number reassignments to consumers who receive excessive nuisance calls, while this option may be helpful to certain Canadians, it could also compound the harm suffered by victims of excessive calls by introducing the burden of having to provide new contact information to their friends, family, and business contacts. Such a practice may also result in subscribers missing urgent or important wanted calls, and may not reduce the number of nuisance calls that they receive. Accordingly, the Commission finds that number reassignment is a generally unreasonable and ineffective solution that should be used only in severe cases.

Conclusion

30. The Commission recognizes that, based on the record of this proceeding, Canadians are generally not satisfied with the current solutions available to block nuisance calls.

31. In general, the options currently available to Canadians are either highly permissive (they allow all calls except those specifically listed) or highly restrictive (they reject all calls except those specifically listed). Further, there are a number of other limitations that diminish their effectiveness.

32. The Commission considers that solutions that (i) are less cumbersome, (ii) offer greater flexibility in terms of level of protection (i.e. low, medium, high) to manage calls, and (iii) rely on community-level information upon which to determine whether the call is a nuisance or not, are needed to provide better protection to Canadians.

33. In light of all of the above, the Commission finds that Canadians do not currently have access to sufficient and effective solutions to protect themselves against nuisance calls.

What solutions could TSPs introduce to better protect Canadians from nuisance calls?

34. Interveners generally agreed that the privacy of Canadians needs to be protected and it is important to restore their trust in the telephony network. However, TSPs generally urged the Commission not to impose any regulatory obligations on the industry.

Proposed technical approach

35. Eastlink and RCP submitted that consumers are in the best position to manage incoming calls using tools such as call management features and smartphone applications.

36. Conversely, the JTF, PIAC, and Shaw argued that TSPs are in the best position to implement effective, sustainable solutions to nuisance calls. PIAC suggested that the responsibility to manage nuisance calls should fall to TSPs since they have the greatest insight and technical ability to do so.

37. Carriers also generally submitted that the investment required to deploy more aggressive near-term solutions could not be justified. Eastlink, MTS Allstream, and Shaw submitted that the transition of more local telephone services to VoIP means that any investments made in legacy telephone systems would not be cost-effective.

38. TSPs submitted that the Commission should request that the CRTC Interconnection Steering Committee (CISC)[13] undertake further study of solutions that are primarily focused on addressing caller ID spoofing.

---

[13] CISC is an industry working group with a mandate to undertake tasks related to technical, administrative, and operational issues on matters assigned by the Commission or originated by the public, that fall within the Commission's jurisdiction.

Approaches to call management

39. Interventions regarding this issue generally focused on two approaches to call management:

    - universal blocking, whereby carriers implement blocking at the network level to prevent calls from reaching any of its subscribers, and

    - opt-in filtering services, whereby consumers subscribe to optional services that would take certain actions to manage suspect nuisance calls on their behalf.

40. TSPs provided a variety of comments on these two approaches, which are outlined below. Moreover, interveners suggested best practices for opt-in filtering services and for notification to subscribers. However, the majority indicated that before these types of solutions are introduced, they should be reviewed by a CISC working group.

Universal blocking

41. A number of parties expressed concern that universal blocking could prevent legitimate calls from reaching their intended recipient. RCP indicated that most TSPs do not universally block nuisance calls on their networks, and that the industry has focused on building robust networks that prevent call blocking due to facility failures or traffic surges.

42. Primus argued that a rigorous verification process would be required to proactively safeguard against incorrectly blocking a number. Several parties also argued that an industry-wide process may need to be established to unblock certain numbers once the illegitimate activity had ceased, or to resolve a dispute in the event that a number is incorrectly blocked.

43. Eastlink, Primus, and trueCall argued that universal blocking, if implemented broadly, would not reflect the distinct preferences of individuals, given that all calls would be blocked at the network level (i.e. affecting all subscribers) and that the blocking could not be customized by the consumer. In this regard, trueCall indicated that 10% of the numbers that its subscribers have on their personal blacklists also appear on other subscribers' personal whitelists.

44. Carriers generally argued that universal blocking is ineffective at combatting nuisance calls from callers who constantly change the numbers that they display on caller ID, which makes it difficult to determine which calls should be blocked. While Shaw agreed with this limitation, it argued that universal blocking is the most efficient and effective solution to combat certain types of nuisance calls. Similarly, RCP referred to its deployment of technology in 2015 to detect and block spam text messages as a solution that could be emulated for nuisance calls.

45. Gosfield North Communications Co-operative Limited (Gosfield) and Shaw indicated that they already maintain internal blacklists of invalid numbers that are

blocked universally at the network level to prevent clearly fraudulent calls from reaching their customers. Shaw indicated that its list is strictly limited to obviously fraudulent calls with a history of high-volume calling. Gosfield indicated that it also blocks numbers based on customer reports of persistent nuisance calls, and that it will reinstate a blocked number if the person or company who owns the number calls to confirm its origin and use.

46. The JTF and CNOC indicated that TSPs are able to identify nuisance calls, including spoofed calls, based on caller ID information, such as cases where the calling party's caller ID

    - matches the telephone number of the person being called;
    - is spoofed with a number that is local to the person being called, in the case of an incoming long distance call; or
    - does not conform to the North American Numbering Plan (i.e. is a non-dialable telephone number [e.g. 000-000-0000]).

47. Shaw advocated for industry-developed and Commission-approved parameters for blocking nuisance calls.

Commission's analysis and determinations

48. Universal blocking is applied at the network level and affects all subscribers. As such, the Commission considers that this solution must only be used where it can be determined that particular calls must not be delivered to any subscribers.

49. The Commission agrees that universal blocking is the most effective and efficient solution to manage nuisance calls in cases where it is possible to accurately identify blatantly illegitimate caller ID spoofing, such as calls that purport to originate from telephone numbers that

    - match the telephone number of the person being called;
    - are spoofed with a number that is local to the person being called, in the case of an incoming long distance call; or
    - do not conform to the North American Numbering Plan (i.e. are non-dialable telephone numbers [e.g. 000-000-0000]).

50. These three specific circumstances account for up to 35% of all complaints filed with the National DNCL Operator in 2015. The Commission considers that universal blocking of these types of calls would be consistent with

    - the UTRs, which require telemarketers to identify themselves and provide a telecommunications number where the originator can be reached; and

- Telecom Decision 2007-48, which states that telecommunications numbers must conform to the North American Numbering Plan in order to be registered on the National DNCL.

51. The use of universal blocking would ensure that Canadians benefit from a minimum level of protection against nuisance calls by fully addressing those that contain caller ID information that is blatantly inaccurate. Such an approach would also not be affected by the limitations of basic calling features, including

    - the need for manual intervention on the part of the individual subscriber;
    - limits on the number of callers that can be blocked or accepted; and
    - the need for in-depth knowledge regarding illegitimate caller ID practices.

52. The use of universal blocking to prevent calls with blatantly illegitimate caller ID information also strikes an appropriate balance between the protection of individual privacy and the need to permit legitimate uses of telemarketing telecommunications.

53. It would not be appropriate, however, to employ universal blocking to manage nuisance calls more broadly since this may lead to unintended and undesirable outcomes. The use of universal blocking to manage suspected unwanted calls could

    - fail to recognize the preferences of individuals to choose which calls they wish to receive;
    - unduly limit the ability of legitimate telemarketers to conduct business;
    - require extensive and complicated industry-wide processes for resolving disputes and unblocking calls that may need to transit through multiple networks; and
    - block legitimate callers who need to conceal their identity (e.g. police or journalists).

54. The Commission considers that TSPs have the greatest insight regarding nuisance calls carried on their network, and therefore considers that CISC is an appropriate forum for the industry to develop practices to universally block calls at the network level. Such practices should include

    - identifying the unintended consequences to legitimate entities, including legitimate telemarketers, and
    - implementing mitigation measures that ensure that any unintended consequences are appropriately managed.

55. Accordingly, the Commission requests CISC to

- identify and develop a comprehensive list of attributes of calls that indicate blatantly illegitimate caller ID information and that can be universally blocked;
- identify potential unintended consequences of universally blocking calls based on the list of attributes identified above;
- as required, develop redress mechanisms to prevent and remediate these consequences when universal blocking is deployed, and approaches for monitoring their effectiveness; and
- provide a report of its findings on the above to the Commission **within 90 days** of the date of this decision.

Opt-in filtering services

56. Interveners commented on two possible opt-in filtering services to manage nuisance calls, namely (i) third-party services, wherein a third party (i.e. other than their carrier) determines whether or not to block nuisance calls on behalf of subscribers to the service, and (ii) carrier-managed services, which provide the same functionality to consumers but are operated by carriers themselves. In addition, Primus and Kedlin provided proposed best practices to follow when introducing opt-in filtering services. These comments are discussed in detail below.

Third-party services

57. TSC indicated that its Nomorobo service has blocked over 60 million robocalls in the United States and is easily deployed through the provision of Simultaneous Ring (Sim Ring), whereby users choose to have all of their calls routed to their home and to Nomorobo at the same time. If Nomorobo determines that a call is a nuisance call, it hangs up on behalf of the subscriber, who only hears a single ring.

58. TSPs generally stated that Sim Ring is primarily supported on VoIP platforms rather than traditional wireline or wireless platforms.

59. Eastlink, MTS Allstream, RCP, SaskTel, and Videotron indicated that deploying Sim Ring for wireline and wireless customers would require significant and costly technical infrastructure changes.

60. Bell Canada submitted that the use of Sim Ring would dramatically increase calling volumes on networks that were designed based upon the principle of one incoming call resulting in one outgoing call. Bell Canada and TCC further indicated that lack of software support, as well as network and database capacity, would be obstacles that call into doubt the technical feasibility of deploying Sim Ring across traditional wireline, VoIP, and wireless platforms.

61. Novus raised concerns about subscriber privacy associated with sending its customers' calls out to a third party for screening, while Primus and Videotron submitted that reliance on a third party to provide automatic call blocking presents a material risk to network integrity in the form of a single point-of-failure (SPOF).[14]

62. Kedlin and Primus argued that a significant shortcoming of Sim Ring is the fact that consumers' telephones still ring at least once.

63. TSPs did not express an intention to rely on Nomorobo, or any other third-party solution that uses Sim Ring, to provide opt-in filtering of nuisance calls.

Carrier-managed services

64. CNOC and the JTF indicated a general willingness to develop and deploy more aggressive call treatment protocols and programs on an opt-in basis to further empower consumers to address and manage nuisance calls.

65. Primus argued that the best technical solutions identify suspected telemarketers in real time and do not block calls, but rather enable consumers to decide for themselves how to deal with nuisance calls. Primus contended that its own Telemarketing Guard service exemplifies this given that (i) telemarketers are identified in real time based on an evaluation of mass-calling behaviour and crowd-sourced user feedback, and (ii) calls from suspected telemarketers are intercepted and redirected to the preferred call treatment chosen by individual consumers.

66. Primus submitted that it was the only Canadian carrier to have developed and deployed a dynamic filtering service across its traditional and digital (i.e. VoIP) home phone platforms, and indicated that the core elements of the Telemarketing Guard platform are technology-agnostic and capable of functioning across VoIP, wireless, and traditional wireline networks. Further, Primus indicated that it would be willing to licence its patented technology to other carriers.

67. Primus acknowledged that its current service does not manage constantly changing spoofed numbers, but indicated that it is currently developing an enhancement to the service to address such tactics.

68. TSPs were generally skeptical about the Telemarketing Guard service's ability to manage spoofed calls, and claimed that they do not have enough information to assess its effectiveness or the time and effort that would be required to deploy the service. However, certain small ILECs anticipated that there would not be any technical limitations to deploying the service if they were required to do so.

---

[14] A failure at a SPOF will stop the entire system from working, be it a business practice, software application, or other industrial system.

69. Several TSPs also raised concerns regarding the scalability of the Telemarketing Guard service. In response, Primus submitted that the effectiveness of the service increases dramatically with the scale of its deployment, and added that the best level of protection for all Canadians would be achieved by enabling the continuous flow of relevant data across carrier networks such that all customers receive the same level of protection.

70. Kedlin indicated that its Call Control solution is available to carriers as an enterprise solution, but did not provide any details regarding its implementation, or the means by which carriers or subscribers would access and operate the service.

Best practices for opt-in filtering services

71. Primus indicated that best practices for opt-in filtering services should include

- interception, rather than blocking, as a default call treatment;
- network-level algorithms to identify nuisance calls;
- crowd-sourced call reporting via star codes;[15]
- providing a choice of call treatment;
- supporting personal blacklists and whitelists that block or allow calls as consumers see fit; and
- ensuring that blocked calls do not ring.

72. Kedlin echoed most of Primus's suggested best practices and further recommended that they include

- an online portal where consumers can manage all aspects of the service;
- blocking based on other attributes (e.g. geographic location or time of day);
- the creation of a national whitelist for emergency-service advisories; and
- the use of standardized star codes for crowd-sourced user reporting and for adding numbers to personal blacklists or whitelists.

Commission's analysis and determinations

73. Services such as Nomorobo and Telemarketing Guard, which allow all incoming calls except those suspected as being nuisance calls to go through, rely on analyses of mass-calling behaviour and users' feedback to infer the likelihood that any given call is a nuisance call. Since these services have access to significantly more information than an individual subscriber, the Commission considers that they are better able to identify nuisance calls.

---

[15] A star code, also known as a vertical service code, is a special code dialed prior to, or instead of, a telephone number that engages some type of special telephone service or feature. Most star codes are two digits in length, and are typically preceded by an asterisk (star).

74. Nonetheless, any given call may be perceived as a wanted call to one subscriber and as a nuisance call to another. As such, and due to the very nature of these services, the calls will not always be treated according to the individual preferences of each subscriber. However, this shortcoming can be addressed by the fact that

    - consumers must choose to subscribe to these services, and could be informed of this limitation as part of the subscription process;
    - these services can be configured to intercept rather than block calls, and to enable the user to define their preferred call treatment; and
    - when offered in conjunction with personal blacklists and whitelists, these services maintain subscribers' ability to exercise their individual preferences for specific callers.

75. These types of services can be employed to enable live telemarketers to reach the intended recipient if the recipient chooses to take the call, but may, for instance, block certain ADAD calls that are unable to respond to a prompt or leave a voice message. Legitimate ADAD calls (e.g. appointment reminders or school closure notifications) that are at risk of being blocked could be managed using a personal whitelist, where available. However, some legitimate ADAD messages could contain critical information, such as community notifications related to emergencies. Accordingly, the Commission considers that opt-in filtering services should include mitigation measures to ensure that legitimate ADAD calls are not blocked.

76. With respect to services that are provided by third parties using Sim Ring, the Commission considers that consumers may benefit from the notice provided by the single ring of their phone when a call is intercepted by a Sim-Ring-type solution. Specifically, this will

    - provide assurance to the consumer that the system is functioning as intended; and
    - in the event of the interception of a wanted call, prompt the user to add the caller to their personal whitelist or to provide feedback to improve the accuracy of the system.

77. The Commission recognizes that services such as Sim Ring will generally be available only on VoIP platforms, given the technical and economic barriers to deploying Sim Ring on traditional wireline and wireless networks. However, the Commission estimates that there are 5 million residential VoIP subscribers in Canada, of which only 1.5 million currently have access to Sim Ring.

78. The Commission is not convinced that the concerns raised by Novus, Primus, and Videotron regarding the use of third parties for call screening, and the associated risks to integrity of their networks or to the privacy of their subscribers, are significant, and could not be adequately solved by carriers. For example, through CISC, carriers have already successfully addressed complex issues such as wireless number portability, which included ensuring that the integrity or security of their networks is not compromised. With regard to the privacy of subscribers, the

provision of this type of service on an opt-in basis would provide an opportunity for the TSPs to inform their subscribers of the system's behaviour and the handling of their personal information, as well as to inform them of the associated risks and to solicit their consent.

79. The Commission agrees with the best practices for opt-in filtering services as proposed by Kedlin and Primus, with one exception – ensuring that blocked calls do not ring. It also considers that another best practice for opt-in filtering services would be to quarantine voice mail messages that the service has intercepted as suspected nuisance calls.

80. Accordingly, the Commission determines that best practices for opt-in filtering service are to include

- identifying in real-time nuisance calls based on an assessment of mass-calling activity and user feedback on that activity;
- not blocking nuisance calls, but rather intercepting and redirecting them without user intervention such that the intended recipient still has access to the call and, to the extent possible, provide a choice of call treatment (e.g. sending intercepted calls to voice mail, requiring the caller to confirm their identity before completing the call), and quarantine voice mail messages from suspect nuisance callers from those left by other callers;
- allowing the subscriber to maintain individual preferences such as those offered by personal blacklists or whitelists or those based on other factors (e.g. geographic location or time of day) and manage all aspects of the service through an online portal; and
- using star codes defined by the North American Numbering Plan Administration for the configuration and operation of the service.

Disclosure and notification

81. Regarding concerns about legitimate calls being blocked, PIAC argued that, as compared to consumers, TSPs have access to much greater amounts of information, and at a more technical level, and that consumers suffer from severe information asymmetry with respect to telemarketing callers, which renders it difficult or impossible for them to effectively manage nuisance calls.

82. With regard to the potential for blocking legitimate or wanted calls, the JTF argued that email filtering tools and services have undergone significant refinement to ensure that in most cases legitimate emails are passed through the network, and that an acceptable balance with regard to blocking of nuisance calls could be achieved similar to that for email, which uses spam filters to quarantine messages that have been identified as suspect spam.

83. PIAC argued that the idea of deciding from the outset that customers would prefer to be subjected to unwanted calls rather than risk missing the occasional legitimate call is paternalistic and not a decision for TSPs to make. PIAC also noted that legitimate calls have rarely been intercepted, and that consumers should have the right to decide whether the benefits of call blocking will outweigh any potential downside. Any vulnerabilities could be minimized by informing consumers through disclosure and notification of any risks associated with the service.

84. CNOC submitted that the Commission should set out clear guidance on disclosure and notice requirements.

Commission's analysis and determinations

85. While CNOC and PIAC provided comments on the issue of disclosure and notification requirements, they did not provide any details as to what the requirements should include. Nonetheless, disclosure to and notification of subscribers are essential to any approach to call blocking or filtering. In the Commission's view, disclosure and notification best practices could be developed by CISC as part of its work to identify and mitigate any unintended consequences related to universal blocking, and TSPs seeking to provide opt-in filtering services could also follow these practices.

86. Accordingly, the Commission requests that CISC develop disclosure and notification best practices as part of the deployment of universal blocking services. These best practices should be included in the report filed pursuant to paragraph 55 above.

Conclusion

87. The Commission expects TSPs to implement universal blocking of blatantly illegitimate calls on their networks based on the findings of CISC, once approved by the Commission.

88. TSPs that provide retail voice services are **directed** to report to the Commission, **within 180 days** of the date of this decision, details outlining the name and description of the opt-in filtering service(s) they offer or propose to offer to their subscribers, including the platform on which the service(s) will be provided, where the service(s) will be available, at what price, and the extent to which the service(s) employ the best practices set out in paragraph 80 above.

89. The Commission is prepared to take further action if it becomes clear that the industry is not taking sufficient measures to protect Canadians against unwanted calls.

What regulatory issues need to be addressed?

Alleged regulatory barriers

90. Several TSPs indicated that the existing rules do not permit them to block nuisance calls on their network. Shaw submitted that section 36[16] of the Act prevents carriers from introducing call-control techniques that would eliminate or reduce nuisance calls from traversing Canadian networks, but suggested that the Commission could authorize carriers to use such techniques pursuant to section 41 of the Act.

91. CNOC and TCC requested clear guidance from the Commission on call-blocking practices in relation to the Act, specifically subsection 27(2)[17] and section 36. In particular, TCC cited the United States Federal Communications Commission's clarification that carriers and VoIP providers are not prohibited from implementing call-blocking technology that can help stop nuisance calls.

Commission's analysis and determinations

92. Contrary to the submissions by some parties, carriers are not precluded under the Act from offering universal call blocking or opt-in filtering services when implemented in a manner consistent with the Commission's determinations herein. Commission approval is, however, required pursuant to section 36 of the Act prior to offering some of these services.

93. In accordance with section 36 of the Act, any conduct by a Canadian carrier that involves the exercise of some power or authority over the content, or has an impact on the purpose or meaning, of the telecommunications carried by it for the public would require Commission approval.

94. By preventing the delivery of a specific call to the intended recipient, call blocking service would have a direct effect on the purpose or meaning of the telecommunications being carried. Accordingly, any such service that does not allow the caller from reaching an intended recipient (as with universal call blocking, for example), approval would be required under section 36 of the Act. This conclusion is consistent with the approach taken by the Commission in Telecom Regulatory Policy 2009-657 (the Internet traffic management practices [ITMP] decision), where the Commission concluded that "where an ITMP would lead to blocking the delivery of content to an end-user, it cannot be implemented without prior Commission approval."

---

[16] Section 36 of the Act states the following: "Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public."

[17] Subsection 27(2) of the Act states the following: "No Canadian carrier shall, in relation to the provision of a telecommunications service or the charging of a rate for it, unjustly discriminate or give an undue or unreasonable preference toward any person, including itself, or subject any person to an undue or unreasonable disadvantage."

95. The Commission intends to approve universal blocking, under section 36 of the Act, for the purposes of preventing nuisance calls that contain blatantly illegitimate caller ID from reaching Canadians. The Commission will do so when it has received and considered the CISC report filed pursuant to paragraph 55 of this decision.

96. With respect to opt-in filtering services that do not block calls, but rather intercept and redirect calls such that the intended recipient has access to the telecommunications, as set out above, the Commission considers that these services can be offered without the requirement to seek approval from the Commission under section 36 of the Act.

Policy Direction

97. The Policy Direction[18] states that the Commission, in exercising its powers and performing its duties under the Act, shall implement the policy objectives set out in section 7 of the Act, in accordance with paragraphs 1(a), (b), and (c) of the Policy Direction.

98. The policy objectives set out in paragraphs 7(a), (b), (f), (g), (h), and (i)[19] of the Act are advanced by the determinations in this decision.

99. Consistent with subparagraph 1(a)(ii) of the Policy Direction, the Commission's determinations in this decision are

- efficient and proportionate to their purpose, given that they are targeted to reducing specific types of nuisance calls while ensuring that the vast majority of legitimate calls are delivered to the intended recipient unimpeded; and

- interfere with the operation of competitive market forces to the minimum extent necessary to meet the policy objectives by providing flexibility to the industry to develop and deploy services that best meet their needs and circumstances, as well as those of their subscribers.

100. Consistent with subparagraph 1(b)(iii) of the Policy Direction, the Commission's determinations in this decision are symmetrical and competitively neutral given that they apply broadly to the entire industry.

---

[18] *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives*, P.C 2006-1534, 14 December 2006

[19] The cited policy objectives of the Act are 7(a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions; (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; (f) to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective; (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.

Secretary General

Related documents

- *Empowering Canadians to protect themselves from unsolicited and illegitimate telemarketing calls*, Compliance and Enforcement Notice of Consultation CRTC 2015-333, 23 July 2015, as amended by Compliance and Enforcement Notices of Consultation CRTC 2015-333-1, 17 August 2015, and 2015-333-2, 5 January 2016

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

- *Unsolicited Telecommunications Rules framework and the National Do Not Call List*, Telecom Decision CRTC 2007-48, 3 July 2007, as amended by Telecom Decision CRTC 2007-48-1, 19 July 2007

Appendix to Compliance and Enforcement and Telecom Regulatory Policy CRTC 2016-442

JTF member companies

9315-1884 Québec inc.
Brooke Telecom Co-operative Ltd.
Bruce Telecom
CityWest Telephone Corporation
Cochrane Telecom Services
CoopTel
Execulink Telecom Inc.
Gosfield North Communications Co-operative Limited
Groupe Maskatel LP
Hay Communications Co-operative Limited
Huron Telecommunications Co-operative Limited
Lansdowne Rural Telephone Co. Ltd.
Mornington Communications Co-operative Limited
Nexicom Telecommunications, a Division of Nexicom Inc.
Nexicom Telephones, a Division of Nexicom Inc.
North Frontenac Telephone Corporation Ltd.
NRTC Communications
People's Tel Limited Partnership
Quadro Communications Co-operative Inc.
Roxborough Telephone Company Limited
Sogetel inc.
Téléphone Milot inc.
Tuckersmith Communications Co-operative Limited
Wightman Telecom Ltd.
WTC Communications