



Décision de Conformité et Enquêtes et de Télécom CRTC 2018-32

Version PDF

Références : Avis de consultation de Conformité et Enquêtes et de Télécom 2017-4, tel que modifié; et politique réglementaire de Conformité et Enquêtes et de Télécom 2016-442

Ottawa, le 25 janvier 2018

Dossier public : 1011-NOC2017-0004 et 8665-C12-201507576

Mesures pour réduire la mystification de l'identité de l'appelant et déterminer l'origine des appels importuns

Dans la politique réglementaire de Conformité et Enquêtes et de Télécom 2016-442, le Conseil a indiqué qu'il amorcerait une instance pour étudier les progrès réalisés sur la question de l'authenticité de l'identité de l'appelant.

*Selon cet examen, le Conseil détermine que les mesures d'authentification et de vérification de l'information sur l'identité de l'appelant pour les appels vocaux sur protocole Internet (IP) devraient être mises en œuvre par les fournisseurs de services de télécommunication (FST) canadiens au plus tard le **31 mars 2019** afin de permettre aux Canadiens de mieux se protéger contre les appels importuns. Les FST sont tenus de rendre compte de leurs progrès. Le Conseil demande au Comité directeur du CRTC sur l'interconnexion (CDCI) de lui présenter un rapport sur les progrès de l'ensemble de l'industrie tous les six mois, le premier rapport étant attendu **six mois** après la date de la présente décision.*

Le Conseil détermine également que l'industrie des télécommunications devrait désigner un administrateur canadien pour la délivrance des certificats qui seraient requis pour l'authentification et la vérification des appels vocaux sur IP.

Enfin, le Conseil détermine que les FST canadiens doivent élaborer un processus de dépistage des appels, et il demande au CDCI de lui présenter un rapport sur un tel processus aux fins d'examen et d'approbation dans les neuf mois suivant la date de la présente décision. Une fois que le Conseil aura examiné le rapport, il déterminera si d'autres mesures sont requises, notamment s'il y a lieu de rendre obligatoire la participation des FST à un processus de dépistage des appels.

Le Conseil est préparé à intervenir davantage s'il devient évident que l'industrie des télécommunications ne prend pas suffisamment de mesures pour protéger les Canadiens contre les appels importuns.

Introduction

1. Dans la politique réglementaire de Conformité et Enquêtes et de Télécom 2016-442, le Conseil a, entre autres choses, conclu que les solutions techniques dont disposaient

les consommateurs canadiens pour se protéger contre les appels importuns n'étaient pas suffisantes¹. Par conséquent, il a pris les dispositions nécessaires pour mettre en œuvre des mesures afin de bloquer, au Canada, tous les appels comportant une mystification manifestement illicite de l'information sur l'identité de l'appelant. Le Conseil a également précisé les modalités selon lesquelles les fournisseurs de services de télécommunication (FST) pourraient et devraient fournir des services facultatifs de filtrage d'appels qui, au nom des abonnés à ces services, intercepteraient et réachemineraient les appels potentiellement importuns. Ces mesures sont complémentaires aux règles concernant la Liste nationale de numéros de télécommunication exclus, ainsi qu'aux règles concernant le télémarketing et l'utilisation de composeurs-messagers automatiques pour faire des appels, collectivement appelées les Règles sur les télécommunications non sollicitées (Règles), et elles font partie d'une approche à plusieurs volets, semblable à celle utilisée en matière de cybersécurité, qui comporte un vaste éventail de techniques d'atténuation et qui offre la souplesse nécessaire pour s'adapter à une menace en constante évolution.

2. Le Conseil fait remarquer que des organismes de réglementation² et des entreprises d'autres pays ont déployé des efforts considérables pour réduire les appels importuns au moyen de diverses mesures et techniques, et que des mesures supplémentaires pourraient être nécessaires pour réduire davantage les appels importuns et fournir aux consommateurs les outils dont ils ont besoin pour se protéger. À cet égard, le Conseil a noté, dans la politique réglementaire de Conformité et Enquêtes et de Télécom 2016-442, que des progrès importants ont été réalisés en matière d'authentification de l'identité de l'appelant depuis la clôture du dossier de l'instance qui a mené à la publication de cette décision, et il a indiqué qu'il avait l'intention d'amorcer une instance de suivi afin d'envisager des mesures additionnelles pour atténuer le problème de la mystification de l'identité de l'appelant³.

¹ Par « appels importuns », on entend les télécommunications non sollicitées qui ne sont pas conformes aux Règles sur les télécommunications non sollicitées (Règles). Les télécommunications non sollicitées qui sont entièrement conformes aux Règles ne constituent pas des appels importuns.

² Aux États-Unis, l'industrie des télécommunications a formé, vers le milieu de 2016, le Robocall Strike Force ayant pour mandat d'étudier des façons d'accélérer la mise en œuvre de mesures pour contrer les appels importuns, et la Federal Communications Commission (FCC) tient des instances sur le blocage des appels et sur l'authentification et la vérification de l'identité de l'appelant. Au Royaume-Uni, l'Office of Communications (Ofcom) a obligé de nombreuses entreprises à participer à un processus de blocage d'appels visant à mettre à jour les listes de blocage d'appels de façon régulière.

³ Il y a mystification lorsqu'un appelant falsifie délibérément l'information sur son identité (c'est-à-dire son numéro de téléphone) qui est transmise à l'appelé dans le but de cacher sa véritable identité. La mystification est souvent utilisée comme un moyen d'amener les appelés à divulguer des renseignements personnels précieux qui peuvent ensuite être utilisés à des fins frauduleuses ou illégales. Il convient de noter qu'il arrive que la substitution de numéros soit utilisée à des fins légitimes, par exemple pour les appels faits par un médecin à ses patients ou les appels faits par les refuges pour femmes.

3. En janvier 2017, le Conseil a amorcé la présente instance de suivi par la publication de l'avis de consultation de Conformité et Enquêtes et de Télécom 2017-4. Dans cet avis, le Conseil sollicitait des observations sur les mesures visant à dépister et à déterminer la source d'un appel importun, ainsi que des renseignements et des observations sur ce qui suit :
 - la mise en œuvre, l'utilisation et l'efficacité des solutions techniques pour authentifier l'information sur l'identité d'un appelant sur les réseaux filaires, sans fil et de communication vocale sur protocole Internet (VoIP) au Canada;
 - la mise en œuvre, l'utilisation et l'efficacité des mécanismes permettant de dépister et déterminer l'origine d'un appel;
 - les obstacles à la mise en œuvre sur lesquels il faudrait agir pour faciliter l'utilisation de ces solutions et mécanismes;
 - les mesures réglementaires qui, le cas échéant, devraient être établies pour garantir aux Canadiens qu'ils peuvent faire confiance à l'information indiquée sur l'identité de l'appelant.
4. Le Conseil a reçu des interventions des parties suivantes : Alliance for Telecommunications Industry Solutions (ATIS); Anthony Rutkowski; Autorité canadienne pour les enregistrements Internet (ACEI); Bragg Communications Incorporated, exerçant ses activités sous le nom d'Eastlink; Canadian Cable Systems Alliance; Canadian VoicePeering Project (VoicePeering); Cogeco Communications inc.; Comwave Networks Inc.; Consortium des Opérateurs de Réseaux Canadiens Inc.; Distributel Communications Limited; Freedom Mobile Inc.; groupe des entreprises titulaires (constitué de Bell Canada, Bell Mobilité inc., Télébec, Société en commandite, et Norouestel Inc.); Independent Telecommunications Providers Association (ITPA); Neustar Inc. (Neustar); Primus Management ULC; Québecor Média inc., au nom de Vidéotron ltée (Vidéotron)⁴; Rogers Communications Canada Inc. (RCCI); Shaw Telecom G.P. (Shaw); TBayTel; TekSavvy Solutions Inc.
5. Selon le dossier de la présente instance, le Conseil a déterminé qu'il devait examiner les questions suivantes dans la présente décision :
 - Existe-t-il des solutions techniques pour rétablir la confiance à l'égard de l'information sur l'identité des appelants et, le cas échéant, quelles sont les mesures réglementaires qu'il conviendrait de mettre en œuvre à cet égard?

⁴ Lors de la présente instance, des observations ont été déposées par Vidéotron s.e.n.c. Toutefois, depuis le 29 décembre 2017, tous les actifs et activités de Vidéotron s.e.n.c. ont été transférés à son affiliée, Vidéotron ltée, et Vidéotron s.e.n.c. a cessé d'exister. Par souci de commodité, « Vidéotron ltée » est utilisé dans la présente décision.

- Existe-t-il des mécanismes pour déterminer l'origine des appels importuns et, le cas échéant, quelles sont les mesures réglementaires qu'il conviendrait de mettre en œuvre à cet égard?

Existe-t-il des solutions techniques pour rétablir la confiance à l'égard de l'information sur l'identité des appelants et, le cas échéant, quelles sont les mesures réglementaires qu'il conviendrait de mettre en œuvre à cet égard?

6. Comme la mystification de l'identité de l'appelant offre l'anonymat, facilitant ainsi la conduite d'activités illégales ou frauduleuses, les Canadiens sont de plus en plus agacés de recevoir des appels importuns. Dans les réseaux à commutation de circuits traditionnels, les appelants n'ont généralement pas la possibilité d'altérer l'information sur leur identité, mais avec l'arrivée des services VoIP, la mystification de l'identité de l'appelant est devenue un problème majeur⁵. De ce fait, les Canadiens ne peuvent plus être certains de l'authenticité de l'identité de l'appelant et ils ne savent plus toujours qui les appelle. Cela nuit à la protection de la vie privée des Canadiens et expose ceux-ci à un risque potentiel.
7. La question qu'il revient au Conseil et à l'industrie des télécommunications de résoudre consiste à déterminer comment rétablir la confiance des consommateurs à l'égard de l'authenticité et la véracité de l'information sur l'identité de l'appelant.
8. L'Internet Engineering Task Force (IETF)⁶ a élaboré une norme technique, appelée STIR⁷, offrant aux FST à l'origine des appels un moyen d'attester la véracité de l'information sur l'identité de l'appelant, permettant ainsi la validation de l'identité de l'appelant. Parallèlement à la norme STIR, l'ATIS a élaboré un cadre de référence, soit la norme SHAKEN⁸, pour la mise en œuvre de la norme STIR dans les réseaux sur protocole Internet (IP) des fournisseurs de services.
9. Conformément aux normes STIR et SHAKEN (STIR/SHAKEN), les FST attestent la mesure dans laquelle l'information sur l'identité d'un appelant donné est digne de confiance. Cette information est transmise au moyen de jetons et est utilisée par l'appelé, ou par son FST, pour vérifier l'authenticité de l'information sur l'identité de l'appelant (c'est-à-dire pour déterminer la mesure dans laquelle l'information sur l'identité de l'appelant est digne de confiance). Ce processus relève d'une ou de plusieurs autorités centrales qui administrent et délivrent les certificats aux FST.

⁵ Dans certains cas, l'information sur l'appelant n'est pas fournie au niveau du réseau, notamment pour les appels provenant d'autocommutateurs privés et d'interfaces à débit primaire utilisés dans le cadre des services d'un réseau numérique à intégration de services.

⁶ L'IETF est un organisme international qui élabore des normes pour l'ensemble des protocoles Internet, c'est-à-dire le protocole Transmission Control Protocol/Internet Protocol (TCP/IP) [protocole TCP/IP].

⁷ « STIR » signifie « Secure Telephony Information Revisited » (nouvelle approche relative à la sécurité de l'identité de l'appelant).

⁸ « SHAKEN » signifie « Signature-based Handling of Asserted Information using toKENs » (traitement de l'information fournie en fonction de la signature au moyen de jetons).

Positions des parties

10. RCCI a fait remarquer que pour plus de 90 % du trafic téléphonique au Canada, l'information sur l'identité des appelants est entièrement authentifiée et attestée, et elle a affirmé que la mise en œuvre des normes STIR/SHAKEN pour ce type de trafic vocal serait redondante. RCCI a de plus suggéré, comme solution de rechange possible aux normes STIR/SHAKEN à court terme, que le Conseil exige des FST qu'ils attestent l'exactitude de l'information sur l'identité de chaque personne à l'origine de l'appel téléphonique. RCCI a noté, toutefois, qu'il serait difficile d'imposer une telle exigence aux utilisateurs d'autocommutateurs privés. Elle a également noté que cette solution de rechange ne permettait pas de régler la question de l'authentification de l'information sur l'identité de l'appelant pour les appels en provenance de l'étranger à destination du Canada.
11. Le groupe des entreprises titulaires s'est dit d'accord avec RCCI et d'autres parties sur le fait que les appels mystifiés ne proviennent généralement pas de FST canadiens. Toutefois, le groupe des entreprises titulaires s'est dit en désaccord avec la solution provisoire de RCCI et a soutenu la mise en œuvre des normes STIR/SHAKEN étant donné que, sans ces normes, les appelés (ou leur FST) ne recevraient aucune information sur la validité de l'identité de l'appelant et seraient donc dans l'impossibilité de distinguer les appels légitimes (p. ex. les appels provenant de FST canadiens de confiance) des appels illégitimes (p. ex. les appels provenant de l'étranger d'appelants dont l'identité a été mystifiée de sorte que les appels semblent provenir de FST canadiens de confiance).
12. De façon générale, les FST et d'autres parties ont reconnu que les normes STIR/SHAKEN pourraient être mises en œuvre, dans l'avenir, afin de rétablir la confiance des Canadiens à l'égard de l'identité des appelants.
13. VoicePeering a suggéré de créer un banc d'essai canadien pour les normes STIR/SHAKEN. L'ACEI a appuyé cette suggestion. Shaw a fait remarquer qu'elle avait l'intention de participer à la mise à l'essai des normes STIR/SHAKEN qui sera menée aux États-Unis par l'ATIS et Neustar.
14. Les parties ont convenu, de façon générale, qu'une entité canadienne devrait être désignée pour administrer et délivrer les certificats aux FST si les normes STIR/SHAKEN devaient être mises en œuvre au Canada. L'ACEI a fait valoir qu'elle pourrait assumer cette fonction. D'autres parties ont indiqué que cette fonction pourrait être assumée par le Consortium de gestion de la numérotation canadienne ou par le Consortium canadien de transférabilité des numéros locaux dans le cadre de leur mandat actuel. Il a également été suggéré qu'une approche technique semblable à celle utilisée pour le protocole HTTPS et le service DNS⁹ dans le domaine Internet puisse être utilisée.

⁹ Le protocole Hypertext Transfer Protocol Secure (HTTPS) encode les données avant qu'elles ne soient transmises par Internet, et le service Domain Name System (DNS) permet de repérer les noms de domaine Internet et de les traduire en adresses IP.

15. Cependant, de façon générale, les FST se sont dits d'avis qu'il était prématuré de mettre en œuvre la technologie STIR/SHAKEN, ou de formuler des observations détaillées sur son fonctionnement et son efficacité, étant donné que les normes STIR/SHAKEN et leurs normes secondaires n'ont pas encore été finalisées et intégrées aux normes d'autres organisations de l'industrie, comme celles élaborées par la GSMA¹⁰, 3GPP¹¹ et CableLabs.
16. Les FST ont également indiqué qu'il n'existe actuellement aucun équipement pour appuyer la mise en œuvre des normes STIR/SHAKEN, et qu'un équipement compatible avec les réseaux IP serait normalement offert d'ici 2020. Les FST ont aussi fait remarquer que les normes STIR/SHAKEN ne pourraient être déployées sur les réseaux à commutation de circuits traditionnels en raison d'un manque de soutien des fournisseurs pour l'équipement sous-jacent.
17. Les FST ont soutenu qu'il serait nécessaire que les normes STIR/SHAKEN soient mises en œuvre non seulement au Canada, mais aussi ailleurs dans le monde, pour que cette technologie puisse être efficace. Il a également été noté que les FST ne pourraient peut-être pas mettre en œuvre l'approche progressive de façon uniforme pour garantir un certain niveau de confiance quant à l'identité de l'appelant, comme le prévoit la norme SHAKEN, et qu'une approche non uniforme nuirait, au bout du compte, à l'utilité de mettre en œuvre une telle technologie.
18. Des parties ont noté que, pour que les consommateurs puissent tirer parti des normes STIR/SHAKEN, les fabricants de combinés devraient mettre en œuvre ces normes de façon à ce que les appareils puissent afficher les renseignements concernant l'authenticité et la véracité de l'information sur l'identité de l'appelant. Des parties ont cependant fait remarquer que ces renseignements ne pourront s'afficher que sur les téléphones IP et sans fil (compatibles avec les réseaux IMS et VoLTE¹²). Il a également été mentionné qu'un programme de sensibilisation ou d'éducation pour les consommateurs pourrait être nécessaire pour veiller à ce que les Canadiens soient capables de déterminer avec succès la mesure dans laquelle ils peuvent faire confiance à l'information sur l'identité de l'appelant.
19. Des parties ont fait remarquer que les normes STIR/SHAKEN ne prennent pas encore en charge l'authentification de l'affichage du nom de l'appelant, et que si cette fonction doit être intégrée à ces normes, des spécifications propres au Canada devront être établies puisque ces renseignements ne sont pas fournis de la même façon au Canada et aux États-Unis. Aux États-Unis, les renseignements pour l'affichage du nom de l'appelant sont fournis à partir d'une recherche dans des bases de données distinctes, tandis qu'au Canada, les renseignements sont fournis par le réseau à l'origine de l'appel. Les parties ont indiqué qu'il s'agit là d'un problème important puisqu'il pourrait ne pas être pris en compte par les fournisseurs d'équipement.

¹⁰ « GSMA » signifie « GSM Association ».

¹¹ « 3GPP » signifie « 3rd Generation Partnership Project ».

¹² IP Multimedia Subsystem, et Voice over Long Term Evolution (voix sur LTE)

20. L'ITPA, appuyée par TBayTel, a déclaré qu'il était trop tôt pour envisager la mise en œuvre des normes STIR/SHAKEN au Canada puisque les petits fournisseurs de services, notamment les petites entreprises de services locaux titulaires (ESLT), ne seraient pas en mesure, à l'heure actuelle, de participer pleinement à un processus du Comité directeur du CRTC sur l'interconnexion (CDCI)¹³ en raison d'un manque de ressources.
21. De façon générale, les parties ont fait valoir qu'il serait prématuré d'imposer des mesures réglementaires pour accélérer la mise en œuvre des normes STIR/SHAKEN.

Résultats de l'analyse du Conseil

22. Le Conseil réitère qu'une approche à plusieurs volets est requise pour réduire le nombre d'appels importuns que reçoivent les Canadiens. En plus des mesures qu'il a déjà prises pour protéger la vie privée des Canadiens, le Conseil estime qu'il est impératif de rétablir la confiance des Canadiens à l'égard de l'information sur l'identité de l'appelant.
23. Il n'est pas possible d'empêcher la mystification de l'identité de l'appelant qui s'observe essentiellement dans le cas des services VoIP puisque ces services ne sont pas fournis dans un environnement géré et clos. Par conséquent, le Conseil estime que les consommateurs doivent disposer d'un moyen de vérifier l'authenticité et la véracité de l'information sur l'identité de l'appelant afin de pouvoir déterminer dans quelle mesure ils peuvent faire confiance à cette information.
24. Le Conseil estime que les normes STIR/SHAKEN sont probablement, à l'heure actuelle, la seule solution viable qui pourrait permettre d'accroître la confiance des consommateurs à l'égard de l'identité de l'appelant. Le Conseil estime également que les normes STIR/SHAKEN auront pour effet d'accroître l'efficacité du service facultatif de filtrage d'appels et du service de blocage à l'échelle du réseau des appels importuns pour lesquels l'information sur l'identité de l'appelant est manifestement illicite.
25. Bien que les appels mystifiés proviennent essentiellement des services VoIP, les consommateurs de tous les types de réseaux sont la cible d'appels importuns. Le Conseil reconnaît qu'il n'est pas possible de déployer les normes STIR/SHAKEN sur les réseaux à commutation de circuits traditionnels puisque l'équipement connexe n'est plus pris en charge par les fournisseurs. Toutefois, le Conseil estime que cette préoccupation est de moins en moins importante pour les raisons suivantes :
- les réseaux des ESLT passent aux technologies de réseau IP;
 - les réseaux mobiles commutés passent à la voix sur LTE (VoLTE), qui nécessite la technologie IP;

¹³ Le CDCI est un groupe de travail de l'industrie ayant le mandat d'entreprendre des tâches liées à des questions d'ordre technique, administratif ou opérationnel sur des sujets assignés par le Conseil ou venant du public, mais qui relèvent de la compétence du Conseil.

- presque tous les réseaux des entreprises de câblodistribution et des entreprises de services locaux concurrentes utilisent déjà la technologie IP ou le feront sous peu;
 - de nombreux FST échangent déjà du trafic au moyen d'interconnexions IP.
26. Malgré ce qui précède, le Conseil s'attend à ce que les FST élaborent et mettent en œuvre des solutions, dans la plus grande mesure du possible, qui permettront d'étendre les avantages des normes STIR/SHAKEN aux réseaux à commutation de circuits traditionnels et aux autres réseaux qui n'utilisent pas la technologie IP, ainsi qu'aux combinés connexes.
27. Il est prévu que les normes STIR/SHAKEN et leurs normes secondaires soient finalisées en 2018. Le Conseil s'attend à ce que les FST canadiens participent activement à la mise en place de ces normes et à la mise à l'essai de l'équipement qui sera créé en fonction de celles-ci pour veiller à ce que les exigences canadiennes uniques soient prises en compte. Bien que la version initiale de ces normes puisse ne pas comprendre de dispositions visant à assurer l'authenticité et la véracité des renseignements pour l'affichage du nom de l'appelant, le Conseil estime que cela n'empêcherait pas les FST de déployer les normes STIR/SHAKEN pour rétablir la confiance à l'égard des numéros.
28. Le Conseil fait remarquer que les réseaux de télécommunication nord-américains sont hautement intégrés et utilisent beaucoup de technologies et de méthodes semblables. Il convient donc de noter que la Federal Communications Commission (FCC) des États-Unis explore activement l'utilisation des normes STIR/SHAKEN dans le cadre des mesures visant à réduire les appels importuns dans ce pays.
29. Le Conseil estime que les FST canadiens devraient être en mesure d'élaborer et de mettre en œuvre des solutions fondées sur les normes STIR/SHAKEN d'ici le 31 mars 2019.
30. Le Conseil est d'accord avec les parties qui ont pris part à l'instance sur le fait qu'un administrateur canadien devrait être désigné pour administrer et délivrer et les certificats à l'appui des normes STIR/SHAKEN. De plus, le Conseil note que l'industrie des télécommunications a réussi à établir des consortiums et d'autres organismes dirigeants afin d'assumer des fonctions semblables, et qu'elle est donc bien placée pour désigner un administrateur canadien des certificats.
31. Par conséquent, le Conseil s'attend à ce qui suit d'ici le **31 mars 2019** :
- les FST mettront en œuvre des mesures pour authentifier et vérifier l'information sur l'identité de l'appelant pour tous les appels vocaux sur IP;
 - l'industrie des télécommunications désignera un administrateur canadien des certificats.

32. Pour permettre la surveillance des progrès de l'industrie, les FST sont tenus de présenter un rapport au CDCI tous les six mois, commençant au plus tard **six mois** après la date de la présente décision, pour expliquer leurs efforts déployés et les progrès réalisés quant à la mise en œuvre de mesures d'authentification et de vérification de l'identité de l'appelant. Le Conseil demande au CDCI de regrouper les rapports des FST dans un seul et même rapport pour le lui présenter ensuite. Les rapports des FST et du CDCI devraient contenir ce qui suit :

- l'état de préparation des FST relativement aux modifications à apporter aux réseaux, s'il y a lieu;
- l'état et les résultats des mises à l'essai d'équipement et de la participation à ces essais;
- des statistiques indiquant ce qui suit :
 - le pourcentage de circuits adaptés pour l'authentification et la vérification utilisés pour le trafic vocal sur IP par rapport au nombre total de circuits à fréquences vocales,
 - le pourcentage mensuel d'appels authentifiés et vérifiés par rapport au nombre total d'appels vocaux,
 - le suivi par niveau d'authentification (c'est-à-dire pleinement digne de confiance, partiellement digne de confiance, aucunement digne de confiance) pour les appels passés aux consommateurs.

33. De plus, le rapport du CDCI devrait faire état de ce qui suit :

- l'état des normes d'authentification et de vérification, comme les normes STIR/SHAKEN et leurs normes secondaires, ainsi que de toute autre norme connexe;
- les exigences propres au Canada contenues dans les normes, ainsi que les efforts déployés pour intégrer ces exigences aux normes appropriées.

34. Le Conseil note que s'il n'est pas satisfait des progrès réalisés par l'industrie relativement à la mise en œuvre de mesures d'authentification et de vérification pour les appels vocaux, il peut envisager d'imposer des mesures réglementaires pour s'assurer que les consommateurs disposent des outils dont ils ont besoin pour se protéger contre les appels importuns.

Existe-t-il des mécanismes pour déterminer l'origine des appels importuns et, le cas échéant, quelles sont les mesures réglementaires qu'il conviendrait de mettre en œuvre à cet égard?

35. Du fait de la mystification de l'identité de l'appelant, le numéro de téléphone qui apparaît sur l'afficheur d'un consommateur ne peut pas toujours être utilisé de manière fiable pour déterminer l'origine des appels importuns. Lorsque l'identité d'un appelant est mystifiée, la seule façon de déterminer l'origine d'un appel est de suivre le chemin emprunté par l'appel du point d'arrivée au point de départ. Ce chemin peut passer par plusieurs réseaux différents.

Positions des parties

36. De façon générale, les parties à l'instance n'ont pas appuyé la mise en œuvre d'un processus de dépistage des appels. Plus particulièrement, le groupe des entreprises titulaires a laissé entendre qu'à l'heure actuelle, il serait préférable de consacrer les efforts aux services de filtrage d'appels et aux processus d'authentification.

37. Si un processus de dépistage des appels devait être mis en œuvre, le groupe des entreprises titulaires s'est dit contre un processus de dépistage pour les services de détail (c'est-à-dire un processus enclenché par le consommateur) puisqu'un tel processus pourrait amener les consommateurs à croire, à tort, que les appels importuns cesseront. Le groupe des entreprises titulaires a également fait remarquer que de nouvelles dispositions tarifaires seraient nécessaires pour un service de dépistage des appels. En outre, le groupe des entreprises titulaires a indiqué que le Conseil devrait établir une condition, en vertu des articles 24 et 24.1 de la *Loi sur les télécommunications (Loi)*, obligeant tous les FST à coopérer dans le cadre d'activités de dépistage des appels.

38. RCCI a noté que le Conseil devrait définir des procédures d'exécution de la loi afin de pouvoir prendre les mesures nécessaires à la suite d'un dépistage d'appels.

39. RCCI, Shaw et Vidéotron ont laissé entendre qu'il serait approprié de confier au CDCI la tâche d'élaborer une méthode détaillée pour dépister les appels dans un environnement à réseaux multiples.

Résultats de l'analyse du Conseil

40. Le Conseil note qu'il a le pouvoir de demander des renseignements aux FST dans le cadre d'enquêtes sur des cas présumés de non-respect des Règles. Il fait toutefois remarquer que l'efficacité de ses efforts pour dépister l'origine des appels importuns est entravée par l'absence d'un processus normalisé. Concernant l'approche actuelle, le Conseil a mentionné ce qui suit :

- elle est souvent longue en raison de l'absence de normes de service convenues et du fait qu'elle comporte des processus manuels qui peuvent dépendre de plusieurs personnes au sein d'un FST donné;

- elle peut donner lieu à des préoccupations concernant les renseignements à échanger, notamment les renseignements personnels;
- elle peut ne pas donner de résultats concluants, même pour les appels provenant du Canada, si les FST canadiens ne conservent pas de dossiers contenant des détails sur l'acheminement des appels durant une période suffisamment longue.

41. Le Conseil a également noté que les FST coopèrent déjà, dans certains cas, pour dépister l'origine d'appels importuns ou malveillants sur leurs réseaux. Cependant, cette approche de collaboration repose sur l'échange volontaire de renseignements entre les FST. Si les FST refusent de coopérer à la demande d'un autre FST, le processus de dépistage prend fin.
42. Le processus de dépistage des appels proposé dans l'avis de consultation de Conformité et Enquêtes et de Télécom 2017-4 pourrait être utilisé par les FST et par le Conseil pour déterminer la source des appels importuns. Le Conseil n'a pas prévu de mettre le processus de dépistage des appels et les résultats de celui-ci directement à la disposition des clients de détail en raison, notamment, du fardeau que cela imposerait aux FST. À ce sujet, le Conseil réitère aussi que, dans le cas d'appels de harcèlement ou de menace, les consommateurs ont accès à une fonction de dépistage des appels payable à l'utilisation. Il leur suffit de composer un code sur leur téléphone pour que s'enregistrent les renseignements sur le dernier appel reçu, renseignements qui peuvent ensuite être examinés par les autorités policières concernées¹⁴.
43. Le Conseil note qu'un processus de dépistage des appels normalisé à l'échelle nationale a été créé au Royaume-Uni¹⁵ et qu'une initiative semblable est envisagée aux États-Unis¹⁶. Le Conseil est d'avis que pour qu'un processus de dépistage des appels fonctionne correctement, la coopération et la participation de tous les FST sont nécessaires.
44. Le Conseil estime qu'un processus de dépistage des appels normalisé à l'échelle de l'industrie est nécessaire pour pouvoir déterminer l'origine des appels importuns. Un tel processus permettra la prise de mesures correctives à la source de ces appels, ou près de celle-ci, contribuant ainsi à réduire le volume d'appels importuns et à améliorer la protection de la vie privée des Canadiens.

¹⁴ La fonction de dépistage des appels n'enregistre que les renseignements détenus par l'entreprise d'arrivée.

¹⁵ Voir les [lignes directrices](#) établies par le Network Interoperability Consultative Committee (NICC) relativement à un processus de dépistage des appels pour l'industrie des télécommunications (en anglais seulement).

¹⁶ Voir le rapport du [Robocall Strike Force](#) présenté à la FCC le 26 octobre 2016 (en anglais seulement).

45. Compte tenu de tout ce qui précède, le Conseil demande au CDCI d'élaborer un processus de dépistage des appels normalisé à l'échelle de l'industrie et de lui présenter un rapport sur ce processus aux fins d'examen et d'approbation dans un délai de **neuf mois** suivant la date de la présente décision. Le rapport devrait contenir ce qui suit :

- une liste des renseignements précis et détaillés dont toutes les parties ont besoin pour procéder au dépistage d'un appel et qui doivent être échangés pour permettre de dépister l'origine d'un appel;
- une description des rôles et responsabilités de toutes les parties devant prendre part au processus de dépistage des appels;
- une description des mesures qui ont été prises, qui seront prises ou qui pourraient être prises pour automatiser le plus possible le processus de dépistage des appels;
- les normes de service concernant la rapidité de l'échange de renseignements entre les parties ainsi que les lignes directrices relatives à la conservation des dossiers contenant les détails des appels.

46. Une fois que le Conseil aura reçu et examiné le rapport, il déterminera si d'autres mesures sont requises et s'il y a lieu de rendre obligatoire la participation des FST à un processus de dépistage des appels.

Instructions

47. Les Instructions¹⁷ mentionnent que, dans l'exercice des pouvoirs et fonctions que lui confère la *Loi*, le Conseil doit mettre en œuvre les objectifs de la politique énoncés à l'article 7 de la *Loi*, conformément aux alinéas 1a), 1b) et 1c) des Instructions.

48. Les conclusions tirées dans la présente décision contribuent à l'atteinte des objectifs de la politique établis aux alinéas 7a), 7b), 7f), 7g), 7h) et 7i)¹⁸ de la *Loi*.

¹⁷ *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication*, C.P. 2006-1534, 14 décembre 2006

¹⁸ Les objectifs stratégiques de la *Loi* énoncés sont les suivants : 7a) favoriser le développement ordonné des télécommunications partout au Canada en un système qui contribue à sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions; 7b) permettre l'accès aux Canadiens dans toutes les régions – rurales ou urbaines – du Canada à des services de télécommunication sûrs, abordables et de qualité; 7f) favoriser le libre jeu du marché en ce qui concerne la fourniture de services de télécommunication et assurer l'efficacité de la réglementation, dans le cas où celle-ci est nécessaire; 7g) stimuler la recherche et le développement au Canada dans le domaine des télécommunications ainsi que l'innovation en ce qui touche la fourniture de services dans ce domaine; 7h) satisfaire les exigences économiques et sociales des usagers des services de télécommunication; 7i) contribuer à la protection de la vie privée des personnes.

49. Conformément au sous-alinéa 1a)(ii) des Instructions, les conclusions tirées par le Conseil dans la présente décision :

- sont efficaces et proportionnelles aux buts visés, qui sont les suivants :
 - réduire l'information trompeuse sur l'identité de l'appelant fournie aux Canadiens afin qu'ils soient en mesure de prendre les mesures adéquates pour répondre aux appels entrants;
 - réduire les appels importuns faits aux Canadiens en déterminant la source de ces types d'appels de façon à ce que les mesures adéquates puissent être prises pour empêcher que de tels appels soient faits à l'avenir;
- ne font obstacle au libre jeu d'un marché concurrentiel que dans la mesure minimale nécessaire pour atteindre les objectifs de la politique en offrant à l'industrie la souplesse nécessaire pour élaborer et mettre en œuvre des mesures de protection qui répondent au mieux aux besoins et aux conditions tant de l'industrie que des abonnés.

50. Conformément au sous-alinéa 1b)(iii) des Instructions, les conclusions tirées par le Conseil dans la présente décision sont symétriques et neutres sur le plan de la concurrence puisqu'elles s'appliquent à l'ensemble de l'industrie.

Secrétaire général

Documents connexes

- *Mesures pour réduire la mystification de l'identité de l'appelant et déterminer l'origine des appels importuns*, Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2017-4, 9 janvier 2017, modifié par l'Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2017-4-1, 2 février 2017
- *Permettre aux Canadiens de se protéger contre les télécommunications indésirables non sollicitées et illicites*, Politique réglementaire de Conformité et Enquêtes et de Télécom CRTC 2016-442, 7 novembre 2016