



[Home](#) > [Public Proceedings](#) > [Transcripts](#)

Transcript of Proceeding

TRANSCRIPT OF PROCEEDINGS BEFORE
THE CANADIAN RADIO-TELEVISION AND
TELECOMMUNICATIONS COMMISSION

SUBJECT:

Review of the Internet traffic management practices of Internet service providers

HELD AT:

Conference Centre
Outaouais Room
140 Promenade du Portage
Gatineau, Quebec
July 6, 2009

Transcripts

In order to meet the requirements of the Official Languages Act, transcripts of proceedings before the Commission will be bilingual as to their covers, the listing of the CRTC members and staff attending the public hearings, and the Table of Contents.

However, the aforementioned publication is the recorded verbatim transcript and, as such, is taped and transcribed in either of the official languages, depending on the language spoken by the participant at the public hearing.

Canadian Radio-television and
Telecommunications Commission

Transcript

Review of the Internet traffic management practices of Internet service providers

BEFORE:

Konrad von Finckenstein Chairperson
Len Katz Commissioner
Suzanne Lamarre Commissioner
Candice Molnar Commissioner
Timothy Denton Commissioner

ALSO PRESENT:

Sylvie Bouffard Secretary
Regan Morris Legal Counsel /
Chris Seidl Hearing Managers
Stephan Meyer

HELD AT:

Conference Centre
Outaouais Room
140 Promenade du Portage
Gatineau, Quebec
July 6, 2009

- iv -

TABLE OF CONTENTS

PAGE / PARA

Sandvine Incorporated 7 / 42
Juniper Networks 65 / 383
Public Interest Advocacy Centre 118 / 730

Ottawa, Ontario

--- Upon commencing on Monday, July 6, 2009 at 0907

1 THE CHAIRPERSON: Good morning. Bienvenue.

2 Bonjour, mesdames et messieurs, et bienvenue à cette audience publique sur les pratiques de gestion du trafic Internet.

3 Le comité d'audition est composé des personnes suivantes :

4 - Len Katz, à ma droite, vice-président des Télécommunications;

5 - Suzanne Lamarre, à ma gauche, conseillère régionale du Québec;

6 - Candice Molnar, conseillère régionale du Manitoba et de la Saskatchewan;

7 - Timothy Denton, conseiller national; et

8 - moi-même, Konrad von Finckenstein, président du CRTC. Je présiderai cette audience.

9 L'équipe du Conseil qui nous assiste comprend notamment :

10 - les gérants de l'audience, Chris Seidl et Stephan Meyer. M. Seidl est directeur, Politiques sur la convergence, et M. Meyer est gestionnaire, Politiques en matière d'évolution des réseaux;

11 - Regan Morris, notre conseiller juridique; et

12 - Sylvie Bouffard, secrétaire de l'audience.

13 Canadians are using the Internet to access a wide range of educational and entertainment content, as well as to communicate with each other. In response to the growth in Internet usage, certain Internet service providers are managing the flow of traffic on their networks. These practices raise a number of concerns, and we launched the current proceeding in November 2008.

14 The Commission has looked into Internet traffic management practices before, but with a very narrow focus. Last year, the Canadian Association of Internet Providers requested that we order Bell Canada to cease throttling peer-to-peer file-sharing applications on its Gateway Access Service. Based on the record of that proceeding, we did not find that Bell Canada had violated the Telecommunications Act and so we denied CAIP's application.

15 Compte tenu de la nature de la plainte, notre examen de la gestion du trafic Internet s'est limité aux seules pratiques de Bell Canada et aux services de gros. Mais les pratiques de gestion du trafic Internet prennent diverses formes, tout comme il existe différentes technologies permettant d'offrir des services Internet.

16 Cette instance nous permettra d'examiner de manière plus générale les incidences de ces pratiques sur les services de détail et de gros. Pour renforcer notre processus public, au mois d'avril, nous avons tenu une consultation en ligne. Les commentaires soumis par le biais du processus habituel et de la consultation en ligne ont été versés au dossier public.

17 At this hearing, we will focus primarily on the following questions:

18 1. What Internet traffic management practices are acceptable and should any be considered as completely unacceptable?

19 2. Should ISPs disclose their practices and, if so, in what form?

20 3. Does the use of Internet technologies for the purpose of Internet traffic management raise privacy concerns?

21 4. Is the application of certain Internet traffic management practices to wholesale services appropriate?

22 5. Is there a need for the Commission to specify what practices are acceptable in relation to wireless service providers?

23 6. What analytical framework should the CRTC adopt in relation to Internet traffic management practices and section 36 of the Telecommunications Act?

24 We will be discussing these questions in order to establish guidelines surrounding acceptable Internet traffic management practices. The guidelines will take into account both the freedom of individuals to use the Internet as they wish and the legitimate interests of Internet service providers to manage their networks.

25 Finally, the Commission has received an application asking that we review and vary our decision regarding CAIP's complaint. This request is presently under consideration. Consequently, parties should avoid referring to any part of the review and vary application during this hearing.

26 I would now ask the Hearing Secretary, Madame Sylvie Bouffard, to explain the procedures we will be following.

27 Madame la Secrétaire.

28 LA SECRÉTAIRE : Merci, Monsieur le Président, et bonjour à tous.

29 Before beginning, I would like to go over a few housekeeping matters to ensure the proper conduct of the hearing.

30 Please note that the Commission members may ask questions in either English or French. You can obtain an interpretation receiver from the commissioner at the entrance.

31 Le service d'interprétation simultanée est disponible durant cette audience. L'interprétation anglaise se trouve au canal 7, et l'interprétation française, au canal 8.

32 When you are in the hearing room we would ask that you please turn off, and not only put on vibration mode, your cell phones and BlackBerry's as they cause interference on the internal systems used by our translators and interpreters. We would appreciate your cooperation in this regard throughout the hearing.

33 We will begin each morning at 9:00 a.m., we will take a break for lunch and a break in the morning and in the afternoon. We will advise you of any changes as they occur.

34 We invite participants to monitor the progress of the hearing in order to be ready to make their presentation on the day scheduled or, if necessary, the day before or after their scheduled date of appearance, depending on the progress of the hearing.

35 Pendant toute la durée de l'audience, vous pourrez consulter les documents qui font partie du dossier public pour cette audience dans la salle d'examen qui se trouve dans la Salle Papineau, située à l'extérieur de la salle d'audience, à votre droite. Le numéro de téléphone de la salle d'examen est le 819-953-3168.

36 There is a verbatim transcript of this hearing being taken by the court reporter sitting at the table on my right,

which will be posted daily on the Commission's website. If you have any questions on how to obtain all or part of this transcript, please approach the court reporter during a break.

37 Please note that the document on the "Issues to be discussed at the 6 July public hearing on Internet Traffic Management Practices" which was sent to all appearing participants on 5 June 2009 is available on the Commission's website and copies are available in the public examination room.

38 I would like to note for the record that the National Union has advised the Commission that they will not be appearing at the hearing. They were Item 3 on the Agenda.

39 We will now proceed with the presentations in the order of appearance set out in the Agenda. Each participant will make their presentation, followed by questions by the hearing panel.

40 Now, Mr. Chairman, we will proceed with Item 1 on the Agenda, Sandvine Incorporated.

41 You may make your presentation. Please present yourself and then you have 15 minutes.

PRESENTATION

42 MR. BOWMAN: Thank you.

43 Chairman von Finckenstein and Commissioners, my name is Don Bowman, I am Sandvine Incorporated's Chief Technology Officer and one of its founders. To my right is Rick Wadsworth, who leads Sandvine's Government Relations and Investor Relations.

44 Sandvine would like to thank the Commission for this opportunity to participate in its review of Internet traffic management practices.

45 Sandvine is a Canadian company and a leading supplier of network policy control solutions, including products designed for Internet traffic management. Our solutions are deployed at over 160 Internet service providers of all network access types in 70 countries. Our goal is to make the Internet better.

46 Based on the Commission's assumptions leading into this hearing, it would appear that Sandvine and the Commission agree on two very fundamental issues to today's discussion.

47 First, network congestion happens.

48 Second, traffic management is necessary in public networks.

49 Congestion is a natural part of a shared network like the Internet and the myriad access networks DSL, cable, wireless and others that comprise it.

50 In times of congestion an unmanaged network is not a neutral network. Inequalities in application design and user behaviour mean that an unmanaged network inherently favours certain applications and their users. Certain bandwidth hungry applications introduce delays into the network that prejudice time sensitive interactive applications like voice over IP and online gaming, which consume relatively little bandwidth.

51 Implicit in recognizing the need for traffic management is the understanding that prioritization between data packets is necessary and part of the IP standards. Prioritization between data packets can occur for a wide variety of legitimate purposes, to prioritize certain traffic in times of congestion; to scrub malicious traffic from a network; to guarantee quality of service for an emergency transmission; to inform a subscriber that he or she may incur extra charges; to boost bandwidth for a file download as part of an on-demand service, and many other uses.

52 In considering whether any guidelines for traffic management are necessary, the Commission may need to decide which of these and other purposes and future purposes yet to be conceived constitute traffic management.

53 Presumably the nature of any guidelines would intrinsically depend on the activities to which they apply.

Prioritization for a given purpose, such as congestion management, can occur through a variety of technical approaches and be supported by a variety of technologies.

54 Given the variety of network architectures between and within access types, the dynamic nature of networks, Internet applications and congestion management solutions, Sandvine submits that any new rules around acceptable traffic management practices, particularly any that are prescriptive, would quickly become outdated and could damage the ongoing health of the Internet.

55 Perhaps a few examples would help illustrate the point.

56 Let's look at one simple difference between network access technologies.

57 DSL is not typically oversubscribed in the upstream direction in the service provider network, but in cable the opposite is true. So in DSL a multi-user congestion management policy may be applied in the downstream direction, while in cable there may be more need in applying a policy to both upstream and downstream.

58 In WiMAX and LTE, two wireless standards, the upstream versus downstream spectrum is dynamic. A single user pushing a lot of upstream traffic can lower the downstream bandwidth of other users. In satellite the round-trip latency is what makes for poor user experience. In this environment you want to ensure that TCP acknowledgment packets are prioritized so that data is not retransmitted by accident due to the loss of acknowledgment.

59 Even within access technology types no two networks are identical and networks change over time, both short time horizons and long time horizons. Congestion exists during peak loads on a network and peaks cannot be predicted in advance.

60 Peak loads may be due to external influences such as a temporary loss in capacity, a world event, such as the music singer dying, or sudden change in application behaviour. A different set of circumstances may demand different approaches. Experimentation is required.

61 As another example, traffic management policies can be based on different traffic characteristics, such as the application being used or the individual user.

62 As Sandvine described in its comments under the public notice, a policy that is targeted at disproportionate users of bandwidth might become more targeted by applying an application-specific policy at the same time.

63 For example, by their nature, voice over IP and online gaming are not bandwidth intensive applications, but

because they are time sensitive their usefulness to consumers is greatly impacted by any delays or loss in their delivery.

64 A policy that targets all traffic of disproportionate users, including time sensitive traffic like VoIP and online gaming, could introduce unnecessary delays in this traffic.

65 Instead, if in times of congestion the policy prioritized all time sensitive applications that are not bandwidth intensive, even for disproportionate users, VoIP and online gaming could be delivered at expected quality level for everybody, while still achieving the congestion management goal.

66 Today operators are using policies that prioritize time sensitive traffic. According to the website of PlusNet, a service provider in the United Kingdom, the purpose of its traffic management policies include to make sure that time critical applications like voice over IP and gaming are always prioritized and to protect interactive applications like web browsing and VPN from non time sensitive download traffic.

67 As a final example, let's consider the implication of changes in network traffic.

68 Sandvine's most recent broadband phenomena report confirmed the ongoing domination of upstream bandwidth by peer-to-peer filesharing, but some of the changes in traffic trends are just as interesting.

69 Not surprisingly, Web and Web media have grown to dominate downstream bandwidth consumption. This category includes, for example, YouTube and other popular video streaming services. But the study was performed before YouTube began supporting high definition video streams. These streams can require eight times the amount of bandwidth compared to a standard resolution video.

70 What will this mean for traffic management policies when HD video is adopted for all top hour video steaming?

71 Sandvine's study also identified a dramatic surge in real-time communications and entertainment applications during the evening periods of peak network utilization when the opportunity for congestion is highest. Online video gaming usage surged the most by over 50 percent, while peercasting and place shifting applications took second spot at over 40 percent growth in bandwidth requirements during the peak.

72 You would be forgiven if you had never heard of peercasting and place shifting. These classes of application were not appearing on Sandvine's customers networks in any significant way the year prior.

73 Slingbox, as an example, is a place shifting application that slings your home TV signal to your Internet device, your mobile phone or your PC, whether you are using it over a fixed line Internet service or mobile.

74 It is not hard to imagine the extreme bandwidth demands of this application and its popularity is only emerging. What traffic management steps will be necessary to maximize quality of experience if this application becomes mainstream? We don't know yet.

75 The Commission has asked whether traffic management practice raise privacy concerns.

76 Sandvine submits that any answer would depend on the Commission's definition of traffic management. It is the uses of technologies that have privacy implications, not the underlying technologies themselves. For example, Sandvine's congestion management solutions don't raise privacy concerns, they don't inspect content because they don't need to in order to achieve their objective. To be clear, our congestion management solutions do not read your e-mail, listen to your voice call or watch your video.

77 Sandvine acknowledges that there are other potential uses of technologies commonly used in congestion management such as deep packet inspection or DPI that may raise privacy issues such as the lawful intercept of Internet traffic or behavioural targeted advertising.

78 The logical next question then is: Do these solutions then fall under the definition of traffic management?

79 Regardless of the answer it is important to distinguish between the use cases and the technology. A camera can be used for taking photos at a birthday party or for surveillance; binoculars can be used for watching -- bird watching or spying. The technology is not at issue, it's how you use it.

80 Nobody questions the legitimacy of cameras or binoculars. Similarly, the use of DPI-enabled devices within a network should not be under question.

81 If the Commission does adopt any guidelines for Internet traffic management practices and their potential privacy implications, Sandvine submits that they should be framed in a manner that is agnostic to the underlying technology so that no particular technology such as DPI is inadvertently prejudiced.

82 DPI is, from a network engineering and architectural perspective, the act of any network equipment which is not an end point of a communication using any field other than the layer 3 destination IP address for any purpose.

83 DPI has been used for years in providing voice over IP services, for providing safe and secure traversal of consumer and enterprise firewalls, for providing network address translation services and for managing quality of service in a network. DPI is also required technology and a critical Internet evolution from IPv4 to IPv6.

84 Mr. Chairman and Commissioners, there seems to be increasing understanding among all participants in this discussion that traffic management is necessary, that an unmanaged network is not neutral.

85 The next natural question to ask then is: What kind of traffic management is acceptable?

86 From its experience Sandvine submits that there are no absolute answers to this question. All elements of the Internet are varied and changing constantly, including the networks themselves, applications and user's demands on the network and the tools available to network providers to manage traffic.

87 In this sort of environment absolute rules are quickly outdated and it is our submission that each traffic management practice needs to be judged individually at a moment in time based on individual results of the network.

88 In Sandvine's understanding, there have been a very limited number of complaints and even lesser number of violations alleging unjust traffic management practices in Canadian Internet. Is anything broken? Is there compelling real-world evidence of the need for new guidelines?

89 But tying service providers hands to deal with the consequences of congestion, malicious traffic or other

network circumstances, additional regulations, particularly if prescriptive, could unintentionally reduce the quality and full variety of our Internet experience today.

90 I would like to thank the Commission for this opportunity to participate in this important discussion on Internet traffic management practices.

91 I look forward to your questions today. Sandvine hopes to be of further assistance as discussions on this topic evolve.

92 THE CHAIRPERSON: Okay. Thank you for your presentation.

93 I read your submission with interest last night and you start off by suggesting that it's wrongly named when we are talking about Internet traffic management. You say we should be talking about congestion management and by using the expression Internet traffic management it's too wide and we have unintended consequences or collateral damages. That's paragraph 19 of your submission.

94 What exactly do you mean by that?

95 MR. BOWMAN: Thank you.

96 So operators today do a wide variety of traffic management practices. These may include security, they may include blocking spam from inbound or outbound access to their network, it may include preventing denial of service attacks from inadvertently or explicitly taking down access networks. These all generally fall under the practice of traffic management.

97 Most of the submissions on the topic here related specifically to the practice of traffic management for the purpose of maximizing the quality of the experience of the users rather than to the broad topic of how to add capacity or measure the need for new capacity or preventing security problems on an the network.

98 So this is what I meant, it may be more broadly framed than needed.

99 THE CHAIRPERSON: I understand that, but you are suggesting in effect we may have -- I mean I'm sorry, I don't understand your whole assumption here.

100 When we set our document we put down the objective and the assumptions. Are you quarrelling with any of those, the objectives that it is to maximize the freedom of Canadians to create applications of the use of the Internet while respecting the legitimate interests of ISPs to manage their networks consistently with privacy and other legislative constraints?

101 MR. BOWMAN: I don't think we are quarrelling with the objectives. I think that there is no accepted definition of Internet traffic management and I think this is -- we are suggesting that Internet traffic management practices with respect to these objectives would be best framed with the specific use case of congestion management.

102 This is our submission.

103 THE CHAIRPERSON: Okay.

104 Now then, you talk also about traffic shaping and session management in paragraph 53 of your submission and then this morning here you have mentioned that the two can be working at the same time, that you can have session management and traffic shaping at the same time.

105 If I understood you correctly, basically session management is you identify the type of traffic that is latency sensitive or jitter sensitive and therefore you give it priority or make sure that it doesn't get in any way compromised. And then, on top of that, you may have traffic management, et cetera, but it's sort of a sequential prioritization?

106 MR. BOWMAN: Sandvine's definition of session management is controlling the number of concurrent typically user sessions present on a network. This is similar to the telephony network. You get a fast busy signal if there is insufficient capacity for a call. So the call is not allowed to enter the network and therefore detract from the quality of all the other existing calls.

107 So in our solutions base session management is one of the techniques. It can be used to delay the ingress of a new video streaming or other application if it would break all of the others.

108 Typically there is more than one concurrent type of technology or policy which is used.

109 Aggregate traffic management is the act of prioritizing all of a type or class. So giving all VoIP as a specific jitter and latency session management is restricting the number of concurrent sessions to control bandwidth.

110 Traffic shaping is a method of reducing the bandwidth of specific applications in order to prioritize others.

111 THE CHAIRPERSON: You quote PlusNet who say:
*"The principles of Plusnet's network management policies
- To make sure that time-critical applications like VoIP and gaming are always prioritised."*

112 How would you do that? How would you always prioritize voice and gaming? That's assuming that's the goal, okay.

113 MR. BOWMAN: Okay.

114 In a technical terminology there's two pieces of technology, there is what's called a shaper or a policer which restricts bandwidth and there is weighted fair queuing or prioritization which controls the order in which packets go into an output pipe.

115 So as an analogy, you know, the door is only one person wide, if I say "Rick, you go ahead of me", that is prioritization. The width of the door is the shaper. If the door was two people wide, him having priority one and me having priority two would have no effect on our speed through the door.

116 So to prioritize voice over IP traffic, it means giving it a higher priority into the queuing mechanism so that voice over IP packets are allowed to precede non-voice over IP packets in order. So this means that they can move ahead in the queue. If there is sufficient bandwidth, the other packets also get through so there is no particular impact to them.

117 So for a service provider to prioritize voice over IP, it first means identifying voice over IP. There are many different types of voice over IP, there is first party VoIP, so the provider may have their own soft switch in the

network; various third-party VoIP, such as Vonage, and so on; and there is over the top VoIP such as Skype.

118 Each of these applications has similar properties in terms of the end user's experience and expectations. They expect a relatively low bandwidth with a relatively low packet loss and a relatively low interpacket variation in delay or jitter. So to prioritize voice over the others means to give it queuing characteristics that match the needs of VoIP.

119 THE CHAIRPERSON: Coming back to your distinction between application prioritization and traffic shaping here, what about which one are you engaging in when you are trying to make sure that time critical applications like VoIP or gaming are always prioritized?

120 MR. BOWMAN: I think it's engaged in both.

121 Typically there would be a shaper or policer which is set to the width of the network so that any packet loss which must occur occurs in our device rather than in the network. So, as an example, if there is a 1 GB connection to an access router, we would have a 1 GB shaper in our device so that the traffic would be groomed in the right order for that. And then into that shaper we would put, in priority order, the packets according to the policy of the service provider.

122 So in this case, as the packets are queued into the access device, VoIP packets would be allowed to precede non-VoIP packets.

123 THE CHAIRPERSON: I was interested that you used this example of games. I thought games, a lot of them, are actually the problem, because they are using P2P and therefore using a disproportionate portion of the bandwidth.

124 MR. BOWMAN: So gaming applications have a couple of different components to them. There is the telemetry, which is how it shares in a multi-user game, where you are right now and what you are doing. This is very real-time and latency sensitive information, but is not very high bandwidth.

125 The second piece of information is there may be side channels related to voice. You may be able to talk to the other participants in the game, so it may have the properties of a voice over IP network.

126 The third component is it may have map updates, which is sending to your PC new virtual worlds and so on to participate in. These are often done via peer-to-peer filesharing, but they are not time sensitive. It's giving your PC updates to the game.

127 So these different components of the gaming have a different requirement or need on the network.

128 THE CHAIRPERSON: And you said that P2P aspect was not time sensitive. And so I could play the games even though that updating is being delayed?

129 MR. BOWMAN: Yes, as long as it is not infinitely delayed --

130 THE CHAIRPERSON: Right.

131 MR. BOWMAN: -- your game will continue to play normally.

132 So as a consumer you value most the telemetry updates being in real time and having guaranteed properties.

133 THE CHAIRPERSON: But since both VoIP and game are time sensitive, if there is not enough bandwidth for both of them you have to make a choice of which one you give preference, don't you?

134 MR. BOWMAN: Yes. So if a network had insufficient bandwidth --

135 THE CHAIRPERSON: Yes...?

136 MR. BOWMAN: -- if it only had two classes of application, VoIP and gaming --

137 THE CHAIRPERSON: Yes...?

138 MR. BOWMAN: -- and you had to make a choice, an operator could choose to give them equal priority, in which case they would degrade equally --

139 THE CHAIRPERSON: Yes.

140 MR. BOWMAN: -- they could do session management, which means that when it becomes insufficient bandwidth new gaming or new VoIP calls would be held off until there was bandwidth, or you could give priority to one over the other. You could say, well, if the network is truly so busy it cannot deliver both VoIP and gaming, then we would prefer to let voice over IP goes through versus gaming, or vice versa.

141 So an operator would have these choices available to them.

142 THE CHAIRPERSON: Presumably the operator would engage the second category, because not making a value judgment, just have a session management.

143 MR. BOWMAN: So different operators have different opinions on how they would like to manage their network.

144 So we provide technology and the guidance on what effect might be achieved, but I don't know how they would all achieve the same goals.

145 THE CHAIRPERSON: But you question the need for us to put guidelines in place. Wouldn't this be a perfect issue of where we should give a guideline? If you are in a situation like that, of the scenario you just painted where you have to choose between two different time sensitive managements, should you be allowed to, in effect, exercise your preference as a network provider or should you employ a neutral device such as session management? It's just the luck of the draw when you sign on?

146 MR. BOWMAN: I think that in order to answer that you would have to recognize that these things evolve over time and some of them may have a fallback mechanism that you are not aware of or they -- you know, your guidelines may become outdated.

147 THE CHAIRPERSON: Oh, I appreciate that, but our whole point is to try to come up with guidelines which, in effect, give you values that you have to apply in the given situation and then you -- we appreciate that situations are infinite, as your submission mentions. You can't possibly predict what will come. Therefore, anything that is specific or technology-based and identified on the state of knowledge right now will be out of date in no time and it would be futile and might be counterproductive.

148 Therefore, what you want to do is isolate what are the key values or objectives, or whatever you want to call them, that have to be achieved, and then suggest: This is the analysis which you should be using in order to determine what you can do.

149 And if somebody complains, obviously, we would rule, saying, "Yes, you acted in accordance with the guidelines," or, "No, you didn't."

150 Would you dispute that that would be a useful activity?

151 I had the feeling from reading your submission that you really feel that guidelines are not required at all.

152 MR. BOWMAN: Sir, for me, it is hard to imagine how the guidelines would be framed.

153 The way that I would frame them would be to maximize the quality of the maximum number of consumers, for the maximum duration of time.

154 If the guidelines were to achieve this in some way, then I think that would be good.

155 THE CHAIRPERSON: Now, you know what we did in the application with CAIP against Bell, which really only dealt with wholesale, but also we were criticized in some quarters about the issue that we, in effect, authorized wholesale network management, rather than dealing with it on a congestion basis. You know, isolate the congestion where it appears, either on part of the network or by the type of activity, and then engage in congestion-specific remedies, which may spring to life when a threat at a certain level is established, and it disappears, or else you put them forward on a historic basis, or an experience basis, or something.

156 Is this possible?

157 I mean, we didn't have evidence then, and you are the expert in this field. Is the technology that far advanced that you can do, in effect, sort of congestion incidents management, rather than wholesale network management?

158 MR. BOWMAN: Over time we continue to evolve our products to make them better, and this is an area that we actively research, congestion detection.

159 We also actively research the impact on the consumer, measuring the true achieved internet quality, a mean opinion score for broadband, if you will.

160 Sandvine's products, as they evolve, have obtained the ability to measure and detect congestion in a simple fashion, and it has gotten better over time. We still have some roadmap ahead of us; however, today there are different techniques which are available. One of them is detecting the amount of bandwidth that is going through a link, compared to its theoretical bandwidth, and there are lab modelled properties of shared access networks which predict, when it hits 70 percent, 75 per cent and 80 percent, that it is entering a near-congestion state.

161 This is one of the techniques we use today. We measure the concurrent throughput and we detect when a change in -- or when the users are trying harder, but it's producing a smaller output. That is our definition of congestion.

162 So I would say that there exists some technology today to do this, but it is still an area of evolution.

163 THE CHAIRPERSON: Is it inexpensive?

164 Presumably, the network operators are very concerned about the economics of doing it, and I assume that part of the reason they would rather do it on a network basis than an incident basis is that it would require an enormous technological investment.

165 Would this have to be disparate, in various places, or could it be done from a central place?

166 MR. BOWMAN: It is highly dependent on the operator's architecture. Different operators would have different deployment methodologies to achieve the same goals, so I can't give a universal answer there.

167 Sandvine is in the business commercially, to make money, so we attempt to price and make our solutions work for our customers.

168 THE CHAIRPERSON: Speaking of economics, is all of this possible to deal with in an economic fashion, rather than in a regulatory fashion?

169 In paragraph 68 of your submission you say: "To be effective and consumer-friendly, access bandwidth charges need a relatively real-time advice, usage and advice-of-charge notification."

170 You sort of suggest that you could have a system by which, when a user goes above a certain level, a message appears that you are now going to be charged extra because you are exceeding your maximum, and hopefully that would discourage you from doing it, and therefore you would obviate the need for traffic management because congestion would go back.

171 It seems like a perfectly sensible way of doing it, let the people who want to use it pay for it, and be discouraged from using excessive loads because of the economy.

172 Does anybody have a system like this in place?

173 MR. BOWMAN: This is an area of active research that I am involved in within the community, which is trying to model economic costs, so that, on a per byte basis, you pay exactly what that byte needs to get through to the network.

174 So if there is sufficient capacity all the way through, it would be free. When there are times of congestion, the bytes that are valued most would pay for it.

175 This would align the interests of the operators -- all operators, including the interconnection operators, the content owners and the consumers.

176 Sandvine doesn't believe today that monthly usage charging has any material impact on congestion. Congestion is a peak time activity. What happens when an operator deploys usage management, in our experience, if it is deployed on a monthly scale, is that the off-peak usage goes down, but the peak still stays where it is.

177 Our point about the advice of usage is that any economic model which deviates from the simple flat rate -- \$40 a month charging that we currently see -- needs to have reasonably good transparency, and one of the techniques in order to get consumer acceptance of it would be that they would have to have full visibility into

when charges were incurred or not.

178 I do believe, in the long run, that economics would be a very strong motivator. It is going to require some changes in how society understands data, and some changes in technology before that vision is fully utilized.

179 THE CHAIRPERSON: So it is, at this point, a Utopian idea. There is nothing in place right now.

180 MR. BOWMAN: It is a little bit closer than Utopia, but it is not a well-achieved norm.

181 THE CHAIRPERSON: But, presumably, there are three aspects. You would need to have the technology, first of all. Secondly, you would need a system of notifying the user. Thirdly, you would need a billing system to back it up.

182 MR. BOWMAN: You would need those three components, and a very agile billing system is something that most wireline operators do not have.

183 But you would need a fourth thing, which is consumer understanding and acceptance.

184 One of the reasons that broadband has grown the way it has is its very fixed and understandable billing model.

185 Consumers don't typically understand the value of a byte.

186 I often use the example when I am talking to mobile customers -- I pull out by BlackBerry and I say, "You know, my BlackBerry is capable of viewing streaming," and everybody is like, "Well, BlackBerrys are great."

187 "And, you know, I am on a volume charge data plan." Well, of course; almost everybody is on a volume charge data plan.

188 And I say, "How big is a streaming video?" And there is never anyone in the room that is able to answer that.

189 Consumers don't understand volume in these terms, so it's going to take some society education, and technology, and billing systems before this becomes an achieved vision.

190 THE CHAIRPERSON: In paragraph 77 of your submission you say:

"Sandvine believes that the disclosure of congestion management practices must balance the need for subscribers to make well informed purchasing decisions and the need of service providers to secure their networks and maintain confidentiality over competitive information."

191 That is a pretty banal statement. I don't think anybody would disagree with it, but how do you do it?

192 What exactly do you have in mind, what do you mean by that statement?

193 Well informed purchasing decisions. How do you get consumers to make well-informed purchasing decisions?

194 MR. BOWMAN: I believe that the disclosure of the general principles of traffic management is required. What we think would be onerous would be requiring an operator to update all of their consumers any time there was a minor change, so if it was very, very specific.

195 Also, if it related to competitive practices, such as the over-subscription ratio of their network, it would be disadvantageous.

196 But, in general, this isn't our area, this is more of a general opinion as a citizen.

197 THE CHAIRPERSON: Let me ask you a question about privacy. I am somewhat surprised that privacy enters this debate at all.

198 Explain to me -- I am obviously a layman in terms of the technology, I don't quite understand why information that is protected by privacy legislation, be it the Privacy Act or the PIPEDA -- why would the network need to have access to any kind of information?

199 This is basically the content. Why, in order to manage the traffic, do you need to have access to the content?

200 I mean, you may have to identify what type of traffic it is, but I don't see why you need to look into it, let alone use it.

201 MR. BOWMAN: Sandvine's definition of content is what the consumer interacts with. It is the specific movie or the contents of the e-mail, and the application we define as the broad category that the user is engaged in.

202 For Sandvine's congestion management solutions, we have no interest in and we don't access the content. In order to do traffic management, it does not say, "This is Spiderman," or, "This is a phone call to your niece." This information is not available for the purposes of congestion management.

203 Privacy enters into the debate because one of the technologies that is used in congestion management is used in other areas. This is called deep-packet inspection.

204 Deep-packet inspection is a broad category of technologies that can facilitate many, many different use cases, one of them being congestion. Others may raise privacy concerns.

205 THE CHAIRPERSON: My friend Len here is a gamer. He uses games all the time.

--- Laughter

206 THE CHAIRPERSON: I don't know whether he does or not.

207 COMMISSIONER KATZ: I'm believing it.

208 THE CHAIRPERSON: His internet service provider finds out that he is using so much that it's causing congestion. Presumably he will do something, maybe session management or some traffic shaping.

209 Why does he have to know -- he knows the fact that Len is a gamer, but why should he be able to use that information, or why should he have to look at what game he plays or something like that?

210 It's a type of activity, and it seems to me that if, by law or by regulation, he is not allowed to use the information that he obtains through deep-packet inspection or whatever -- I cannot for the life of me see that for any legitimate person, a reason the ISP should need to know what kind of games he plays or how often he plays or something, all they need to know is he is a gamer, he uses a lot of games and that is impairing the integrity of our network.

211 Am I wrong here, am I missing something?

212 MR. BOWMAN: In aggregate, knowing information like duration of session and how many people engage in

activities is very valuable for the purposes of capacity planning and building the network to meet the needs of your consumers.

213 So, it's -- the more an operator knows in that sense the better quality of service they can provide for a given capital investment.

214 As to the specific games, it rarely needs to go to this level. What you normally need, or it's useful if you have is information on duration of session, the utilization of the network during those sessions, so the band width consumed, the number of people engaging in those activities and the trending over time.

215 Are more people doing gaming, or is it the same number of people doing gaming but it's causing an increase in network utils -- utilization.

216 THE CHAIRPERSON: Yes. But as long as that information, whatever it is, he uses it only for the purpose of traffic measurement, he doesn't impart it, he doesn't use it for marketing or something.

217 I don't see that there is any invasion of privacy at that point, it's purely -- if I understand you, it's used for the technical management of the network.

218 MR. BOWMAN: So, this is what Sandvine, we market our products for, yes.

219 THE CHAIRPERSON: Yes. What about wireless carriers, the term used is use of ITMPs. In the wireless environment rather than a wire environment, is there any difference, is there anything that is of qualitative difference that we need different rules for wireless environment and wire line?

220 MR. BOWMAN: There are some major differences that relate to both the technology, but also to the business model.

221 So, today most wireless operators have a slightly different charging scheme than the wire line operators and this, in turn, has a control on the average capacity of their network but not the peak.

222 Wireless operators, by the nature of their technology, they suffer from a few problems such as mobility. So, I use the example, Michael Jackson died the other day, the hospital that he was taken to had thousands of people outside of it each with a cell phone, this was an unanticipated peak load on the network. This is a specific to wireless problem and it may lead rise to temporary situations that are unanticipated but not long term.

223 Secondly, wireless is switching to data. Over time the voice segment of it is becoming less and less. The wireless standard such as LTE and WiMAX anticipate an entirely data-based network in which the voice is fully converged but the primary use case is data.

224 When they arrive at this point in time, the consumers are going to use it in largely similar fashion. The over subscription ratio, which is the amount of band width available as a ratio to what's used, can be quite different in wireless because it's based on physical properties of radios.

225 Also the ability of one user to impact another on wireless is very high compared to wire line. I gave the example how in WiMAX and LTE the upstream and downstream spectrum can dynamically shift, so one user's upload can impact another user's download.

226 So, there are strong technical differences between these.

227 In a wireless network, there is largely similar needs for traffic management, however, today wireless data is not so evolved that it has become a significant commercial problem, it is on the cusp of that; in some markets it has passed it, in others it has just started.

228 THE CHAIRPERSON: I guess I don't know what your answer was because -- but I want to know is, do we need special rules for wireless or not?

229 MR. BOWMAN: I think that there may be a reason in a wireless network based on its technology that you may need to have additional tools available.

230 THE CHAIRPERSON: Okay. Now, you mentioned upstream and downstream and in your presentation you also suggest that the ADSL we have an upstream problem and the cable company downstream or vice versa, I forget which way it was.

231 But I mean, that's just a question of configuration and use of the networks; isn't it? I mean, the ITMPs you would be employing would be the same whether it's upstream or downstream, or do you use different ITMPs for one or the other?

232 MR. BOWMAN: You would use different ones because the nature of the traffic in each direction on a network is quite different.

233 So, the upstream direction is information the consumer publishes to the network.

234 THE CHAIRPERSON: Yes.

235 MR. BOWMAN: And is a much smaller subset of information than information the consumer consumes from the network.

236 So, today a very small number of consumers would stream video out of their home, but a very large number would stream video into their home.

237 It's -- ADSL and cable have a very specific technology choice difference in there and the operator can't change that. Over time their vendors can make modifications, but they can't change it.

238 So, the tools that -- the techniques and tools that are used in a cable network may be different than an ADSL.

239 There's a secondary difference which is there's facilities in the access network which can assist in traffic management. For example, in cable there's a technology called packet cable multi-media. What this allows us to do is to move the prioritization in the upstream direction in to the user's house, we're able to signal their modem in the upstream direction which we're not able to do in ADSL.

240 So, as a consequence, we use slightly different techniques in cable and DSL, both from the technology choices that they have used and also from the applications the consumers use on those networks.

241 THE CHAIRPERSON: Yes. That's the technology. I have no doubt they are different, but I was talking about

terms of objective and what you're trying to achieve, et cetera.

242 It's the same in either direction; isn't it? Whether it's uploading or downloading, you're trying to make sure that the time sensitive applications do not get impaired by the others and that to the extent that time sensitive applications require upstream from others, they get it and vice versa.

243 MR. BOWMAN: I would agree, they have similar objectives but they use different practices to achieve those objectives.

244 THE CHAIRPERSON: Okay. Thank you.

245 Those are my questions.

246 Len?

247 COMMISSIONER KATZ: Thank you, Mr. Chairman. I've got a series of questions.

248 I'm going to start with something you said in your opening remarks and I think in a comment to the Chairman you stated, peak stays where it is and you also stated, peaks cannot be predicted in advance.

249 You mentioned the Michael Jackson situation and, obviously, unique world events are unique by definition, but peaks can be forecast, peaks have always been forecasted, in fact every ISP, every network provider builds their network based on peak. Is that not the case?

250 MR. BOWMAN: Yes. There's no Erlang model for data, but operators do forecast the reasonable peaks they expect, but an event such as a cable cut or a sudden flash mob or something they cannot predict.

251 So, my point there was that peaks change on both a short and long-term basis. The long-term ones are predictable in the meta sense.

252 COMMISSIONER KATZ: And the longer term peaks are the ones that cause infrastructure costs to be expended. I mean, you know your peaks are from six to eight o'clock at night in the case of perhaps the Internet or whatever and, therefore, when you build capacity you're recognizing that you have congestion at that period of time, even though you're putting in network capacity in for 24 hours seven days a week, the reality is you're trying to overcome a certain competitive need at the peak because that's where your quality of service is being impacted.

253 MR. BOWMAN: The peaks are not always at those times. There are events, like the Obama inauguration that occurred during the day. Peaks can also be -- like the Vancouver Olympics, the peak will be substantially different than the -- for the wireless carrier there.

254 But, yes, in general operators build their network to peak capacity by capital investment to achieve a given quality objective.

255 COMMISSIONER KATZ: Does Sandvine develop models and techniques to identify and forecast when those peaks are going to happen as part of your services?

256 MR. BOWMAN: Our data is used in the modelling of that. The example I gave earlier about knowing the number of sessions and duration of session for gaming versus VOIP, we try to give an operator tools to predict not only the peak capacity but the peak capacity that is elastic and inelastic; that is, the peak capacity that has a very high quality guarantee required versus a medium versus small so that an operator can use that as part of their capacity planning and modelling process.

257 COMMISSIONER KATZ: Okay. So, you sell those services to network providers?

258 MR. BOWMAN: We sell products that they use to achieve this, yes.

259 COMMISSIONER KATZ: How does the network provider turn what they pay to you into value for them, because obviously there's a value proposition there. So, how do they turn that into something that creates shareholder wealth?

260 MR. BOWMAN: Sure. So, what our customers do is they try to maximize the quality of experience of their consumers because it relates to specific cost in churn. So, churn is leaving one operator for another. One of the reasons for churn is a perceived or real quality degradation of service, so that would cause you to pick up the phone and call your current service provider and cancel.

261 So, with our products they're able to help measure quality events that would lead to churn and they're better able to predict capacity, leads to better overall quality of the network.

262 But third is Internet traffic management itself can lead to better quality, in the sense that when the network does become congested or over subscribed, protecting the experience of the interactive applications can in turn give the user a better quality of experience and likelihood of churn is reduced.

263 This is one of the primary business propositions to our customers.

264 COMMISSIONER KATZ: Okay. So, when they have that information and they're able to utilize it, I want to come back to something that I think you mentioned earlier with the Chairman as well and, that is, to what extent does that data get utilized? And I think you used me as an example of a gamer.

265 To what extent does the network provider need to know that it's Len Katz who's running the gaming system and using it, or that between whatever times of the day or week there is high incidence of a number of people that are gaming and, therefore, they need to do something in order to counter that congestion or else they will start losing customers?

266 Like, to what extent is it customer specific or broad categories of users?

267 MR. BOWMAN: So, there's a couple of different examples here. One of our products measures the achieved call quality of voice over IP and it can generate an alarm on a specific user when they're not achieving some service level agreement.

268 So, in this case it would be a -- it would identify the specific user and the time that the problem occurred.

269 Other measurements occur in aggregate. The aggregate needs to be specific enough to matter but usually it is not specific to a user level. So it could be specific to a piece of access equipment or sometimes aggregates go across the other way. It is business versus residential or the 4-megabit versus 6-megabit tier.

270 Within these aggregates, you are predicting the capacity required, the trending upwards or downwards, the

number of users. So to the extent that it is an individual user, it is typically based on a trouble ticket or problem or security event or abuse ticket or something like this. This is typically why they use information on an individual basis. Typically they use information on those aggregate bases for the other network planning purposes.

271 COMMISSIONER KATZ: So if I called up and said I had a problem yesterday in the evening with playing my game, they would be able to go onto their system and say, Mr. Katz, you have been playing whatever game it is religiously for hours and hours and it uses an awful lot of bandwidth, and as a result of that, we had to slow you down? They have that capability online real-time to tell me that?

272 MR. BOWMAN: Not exactly yet. It would depend on (a) how they configured our equipment. There would be a capital cost of keeping that level of detail, which is not common. And (b) we don't have the trouble ticketing or help -- you know, the scale of the consumer asking the question would challenge us today.

273 COMMISSIONER KATZ: But the capability will be there?

274 MR. BOWMAN: I would assume that there would be the ability for an operator to record quality information about the service as delivered and then, on request of the consumer, access it. But we don't currently have this capability.

275 COMMISSIONER KATZ: Once we do have that capability, could the network provider then say, if you want a higher quality of service in order to continue, we will have to upgrade your price plan or your consumption usage to a higher cost, in which case we can guarantee you a certain level of speed and throughput?

276 MR. BOWMAN: To the extent that they offered a tariff rate plan that was more appropriate for you, then I guess yes.

277 COMMISSIONER KATZ: Okay. Do you know to what extent the quality of service measurements or obligations of the network provider are actually passed through to consumers, to what extent consumers know what quality of service level they are getting?

278 MR. BOWMAN: I think consumers interact in a much more subjective manner. You know, if I put you in front of a keyboard and said, is this a good Internet quality of experience, think of what you would use. You would say, well, I didn't get a lot of spam on it and my voice call seemed to complete and my banking Web page was fairly snappy and my corporate VPN was able to connect. They use a set of subjective measures like that.

279 This is one of our technical challenges right now, is to try to build a model between very specific things we can objectively measure, such as latency, loss and jitter and so on, and bring that into the framing of how a consumer would see that service.

280 I think today the concept of quality of service on the Internet as a whole is improving but is still fairly nascent. You know, people know whether streaming works or not, whether it is constantly rebuffering or plays smoothly. That is how they see quality of experience.

281 COMMISSIONER KATZ: One of the things that I have noticed is that carriers, never providers, market their services with speeds up to something --

282 MR. BOWMAN: Yes.

283 COMMISSIONER KATZ: -- and that up to can be up to that level but it can be substantially lower than that as well.

284 Is there a way, is there software or controls in place that would create an environment where they would guarantee a minimum level for a price point so that you would never drop below that level because they could monitor the network and guarantee a minimum level of throughput?

285 MR. BOWMAN: Absolutely. This is done for business users today. You can achieve both a maximum and a minimum with network engineering.

286 COMMISSIONER KATZ: Okay.

287 Those are my questions, Mr. Chairman.

288 THE CHAIRPERSON: Suzanne, you have questions?

289 COMMISSIONER LAMARRE: Merci, Monsieur le Président. I have a couple of questions.

290 I want to go back, and it is sort of a follow-up also to the answers you just gave Mr. Katz and the answers you provided to the Chairman when he questioned you with regards to paragraphs 66 and 68 in your submission about the development of technology and you answered mostly talking about the research that is being done right now in modeling the economics and the value of the bit rates. That answer is clear.

291 What I did not understand or get from your answer is the following. Is it possible right now with the technology or is it close to being possible to be able to actually meter the data flow?

292 MR. BOWMAN: There are operators today who provide a metered pay-per-bit service plan. In fact, in Canada, the majority of them do this today.

293 COMMISSIONER LAMARRE: Okay. So it does exist. Okay.

294 Now, you have mentioned a couple of times in your presentation the expression "malicious traffic." Can you tell me from whose perspective we should be defining malicious traffic?

295 MR. BOWMAN: Sandvine frames everything in terms of the consumer's experience. So in the limit, a perfect product would prevent any packet from arriving to your house that you didn't want, you didn't solicit.

296 So malicious traffic can be spam, it can be a worm or a virus, it could be unsolicited pornography, it could be anything. Now, that is a pipe dream to get down to the packet level here.

297 But secondly, malicious also has an impact on an operator. Today there is a problem called a distributed denial of service attack where many PCs somewhere in the world attack one or a small number in a network and that may in turn impair or entirely destroy the quality of experience for all users served on the same access router.

298 So this is one of the common problems today, that this malicious traffic, it has no value to the consumer that it is going to and they would prefer it not to arrive and it may in turn have an economic or quality cost to an operator.

299 COMMISSIONER LAMARRE: So from your corporation's point of view, malicious traffic, as you mentioned at the beginning of your answer, is that you define it from the consumer's point of view?

300 MR. BOWMAN: Yes.

301 COMMISSIONER LAMARRE: Okay. On the privacy issue, in your presentation you make the point that -- you said, for example:
"Sandvine's congestion management solutions don't raise privacy concerns." (As read)

302 That's your statement. And you say:
"They don't inspect content because they don't need to in order to achieve their objective." (As read)

303 But does the equipment you sell and the congestion management solution that you sell, do they have the capacity to do that?

304 MR. BOWMAN: We do not currently have the capacity to detect and record content. So in this sense content as I have defined it is what the consumer interacts with. It is the movie "Spiderman" or it is the e-mail from your niece. We act at the application level, the broad category level. This is our current capacity today.

305 COMMISSIONER LAMARRE: Okay. And when you are talking about the value of aggregated information in order to be able to understand the traffic and then manage it in a better fashion, in order to get the aggregate info, you need to first get the individual information, don't you?

306 MR. BOWMAN: Yes. This is done automatically inside our device. Our device records a set of information in real-time in its memory but then it logs on specific time intervals, aggregates of that, which is what the operator uses for reporting.

307 So the very specific information is not available to any person, it is only available to the machine. The aggregated information is stored in a relational database for later reporting purposes.

308 COMMISSIONER LAMARRE: But the machine can actually store that information and it is accessible to either a system administrator or --

309 MR. BOWMAN: No. It is real-time in the process of doing this. It makes its decisions and it forgets them in real-time.

310 COMMISSIONER LAMARRE: So it is being dropped?

311 MR. BOWMAN: That is correct. It is not stored anywhere.

312 COMMISSIONER LAMARRE: Okay.

313 MR. BOWMAN: We don't have the capacity to do that today.

314 COMMISSIONER LAMARRE: Okay. And just on your statement that -- you say that the Commission has asked whether traffic management practices raise privacy concerns and you submit that any answer would depend on the Commission's definition of traffic management.

315 Well, privacy being a fundamental right, shouldn't traffic management adapt its definition to the privacy issue instead?

316 MR. BOWMAN: Sure.

317 COMMISSIONER LAMARRE: Okay. Thank you. Those are my questions.

318 THE CHAIRPERSON: Tim?

319 COMMISSIONER DENTON: Thank you, Mr. Chairman. Good morning, gentlemen.

320 We know that the Internet is based on a best-efforts model and certain forms of traffic are less sensitive to jitter or latency than others. Is this the reason that you say that an unmanaged network is not neutral?

321 MR. BOWMAN: When the Internet was originally framed, all parties involved had a common shared interest in the success of it and there were no selfish actors. As the Internet has evolved to have more and more parties on it, we see actors that are emerging that have a self-interest.

322 So the self-interest may be related to an application. So somebody may program an application to try to consume as much as they can because it gives a better experience for their users and then they come at an expense to others.

323 So we say that an unmanaged network is not neutral in the sense that it may achieve the goal of a small number but not all.

324 COMMISSIONER DENTON: Okay. Fair enough. Because the Internet functions on a certain social premise which is no longer accepted by all actors?

325 MR. BOWMAN: One of the key protocols on the Internet, TCP, was based on a generic design principle that each TCP connection would achieve relatively equal bandwidth when there were many connections present.

326 Some application providers took advantage of this and they found that by opening more connections they were able to achieve a larger pro rata share of the bandwidth with throughput. These applications therefore shifted the burden so that people who didn't use these applications were disadvantaged.

327 But yes, the fundamental best-effort nature plus the cooperative nature of the original protocols is what leads to this situation.

328 COMMISSIONER DENTON: That is why I was interested in your point. You say:
"The prioritization is a part of the IP standards." (As read)

329 MR. BOWMAN: Yes.

330 COMMISSIONER DENTON: Is this so, where and are routers configured to handle that prioritization?

331 MR. BOWMAN: Prioritization on the Internet is done in a number of different techniques. Probably the oldest one is called IP type of service or differentiated services code point. So what this is is this is a mark that can be put on a packet and at each hop through the network, each router-to-router interconnection, it can be used to weight the priority of those packets.

332 So today this would be used for Voice over IP. There is a commonly held mark in there. It is very commonly used on enterprise networks within service provider networks or other techniques used such as MPLS.

333 MPLS is a way of providing guaranteed bandwidth, to the earlier question through traffic engineering you can make a connection between two points which says it has no less than 10 megabits available any time and no more than 100 megabits.

334 So, this would be another technique that's part of the broad portfolio of IP Standards. So, those are two primary ones.

335 COMMISSIONER DENTON: Okay. It's perhaps unfair to quote you back what you were saying if there were a principle that we would seek to enshrine, it would be maximum equality over the maximum number of consumers for the maximum amount of time.

336 Let's just go over this for a moment. What would the quality mean in that sense?

337 MR. BOWMAN: So, maximum quality, so quality is the subjective method.

338 COMMISSIONER DENTON: Is it equality or quality?

339 MR. BOWMAN: Quality.

340 COMMISSIONER DENTON: Thank you.

341 MR. BOWMAN: I don't think that equality would necessarily achieve quality.

342 COMMISSIONER DENTON: That was my point, but --

343 MR. BOWMAN: It's quality.

344 COMMISSIONER DENTON: -- carry on.

345 MR. BOWMAN: So, it's quality. So, if I was to give every consumer in the world a piece of paper and tell them to write down what they objectively or subjectively perceive their quality of experience on a score from one to five and collect all those cards and average them, that main opinion score would be to deliver quality.

346 We are seeking a technical means to measure it in such a way that it has a strong correlation to how those consumers would write this number down.

347 Today, we have individual point metrics related to DNS round trip time and latency device over IP, latency loss and jitter band with a kodak to web page average time to load responsiveness and so on.

348 Each of these individual metrics we are then seeking away to merge into one number. So, we view that this would become a very powerful capacity planning tool. Operators will start to eventually build their network to a constant quality rather than projecting feature bandwidth requirements.

349 COMMISSIONER DENTON: Okay. So, that's what you, Sandvine, are up to in terms of trying to generate a number that would -- or a metric that would work like that?

350 MR. BOWMAN: This is our area of research, yes.

351 COMMISSIONER DENTON: Okay. Finally, you say -- you were suggesting that we confine our concerns to congestion.

352 Is congestion the essence and is it really the only thing that we need to be concerned about in the matter of traffic management?

353 MR. BOWMAN: For the purposes of internet traffic management, I would define it for the practices that are used to deliver a better quality during times of congestion. I think that would exclude the security and other components that I brought up earlier.

354 COMMISSIONER DENTON: It would exclude security as a concern.

355 MR. BOWMAN: I would personally would do this, yes.

356 COMMISSIONER DENTON: Thank you.

357 MR. BOWMAN: I think otherwise it becomes an unbounded problem statement.

358 COMMISSIONER DENTON: Thank you. Those are my questions.

359 THE CHAIRPERSON: Okay. Thank you very much. Okay. You had one question?

360 COMMISSIONER POLNAR: Thank you. I would just like to follow up because I too have been following this and interested in your notion that we should be concerned only with traffic management for the purpose of congestion.

361 Packet prioritization has the potential to impact other users on the internet. Correct?

362 MR. BOWMAN: Well, yes. Packet prioritization affects the order or speed you receive your packets in which, in turn, affects users.

363 COMMISSIONER POLNAR: Okay. And so, when packet prioritization is done for purposes other than congestion management, why would we not be considering that as part of this hearing?

364 If we go back to our objective and our definitions as to -- and I'll just pull this out again -- the objective to maximize the freedom of Canadians to create applications and use the internet, while respecting the legitimate interest of ISPS to manage their networks, they manage their networks, they prioritize packets for more reasons than just congestion.

365 So, why would we focus ourselves solely on the purpose of congestion?

366 MR. BOWMAN: I would say that we don't know all the use cases today. You know, our position in what we are experts in relates to a certain set of areas, you know. I am familiar with security use cases, I am familiar with congestion management use cases, I am familiar with some of the capacity planning.

367 I am personally not familiar with all of the potential use cases that are here.

368 So, you know, I think it is up to the Commission to make a decision here, but my suggestion is that there would be more success on focusing on a specific use case than on very broad.

369 I think if traffic management as a term comes to encompass every aspect of how an operator runs every aspect of their network, it would become very difficult to complete.

370 COMMISSIONER POLNAR: Would it be fair to say that traffic management could include every purpose for prioritizing packets amongst different users of the public internet?

371 MR. BOWMAN: So, I would say I don't know the answer to how we would define that, but I would say that,

you know, an operator may have service plans. You asked the question earlier about guaranteed minimum bandwidth. That is a form of prioritization.

372 In our marketing, we would view that as service creation, you know, for this price I would sell you a service which has this guarantee. I wouldn't view that as traffic management per se. I would view it as service creation personally.

373 I mean that's how our company would market that solution. But it is prioritization when you do that.

374 It's similarly prioritization how you build capacity in an area. That's a form of implicit prioritization and I too wouldn't view that as traffic management personally.

375 COMMISSIONER POLNAR: That's my question. Thanks.

376 THE CHAIRPERSON: Okay. Thank you very much. I appreciate your intervention.

377 We will take a ten-minute break.

378 MR. BOWMAN: Thank you very much.

--- Upon recessing at 1018

--- Upon resuming at 1030

379 THE CHAIRPERSON: Okay. Madame la secrétaire, commençons.

380 LA SECRÉTAIRE: Merci, monsieur le président.

381 I would now invite Juniper Networks to make its presentation.

382 Appearing for Juniper Networks is Mr. Stevens. Please introduce your colleague and you will then have 15 minutes for your presentation.

PRESENTATION

383 MR. STEVENS: Thank you very much. Good morning and thank you for the opportunity to present today in front of the Internet Traffic Management Practices hearing.

384 My name is Scott Stevens. I am the Vice President Technology for Juniper Networks. To my right is Doug Linder. He is our Assistant Engineering Manager for Canada.

385 I have a brief presentation we wanted to go through as we begin our conversation today.

386 Juniper Networks is a company that has been in existence since 1996. We manufacture telecommunications equipment, routers, switches, fire-walls in support of Carrier Networks, Enterprise Networks and Public Service Networks around the world.

387 We have done business in almost every country of the world today and obviously do quite a bit of business within Canada.

388 We focus very aggressively on building networks and having the capacity to build networks that are fast, reliable and secure. We believe it's in everybody's best interest to have an infrastructure that's fully capable and able to innovate and differentiate what occurs across the background.

389 And we spend roughly three quarters of a billion Canadian a year on research and development to make sure that we have the technology and the capabilities available to all of our customers to make the most efficient use of the networks that they build.

390 In our submission, we talked about a couple of different ways to look at traffic control methodologies. We mentioned a concept called "light listing and black listing". Now that is not to construe that one is good and one is bad. It has simply been a very simple way to articulate two views.

391 Fundamentally, light listing is the approach of looking at applications, services or users that require specific enhanced treatment across the network. As we have just heard from Sandvine, a lot of conversations are on Voice Over IP, for example.

392 In many countries a replacement voice service that replaces the public telephone network offered by a carrier must have the equivalent levels of performance and security, especially around concerns such as 911 and that, obviously, forces some level of white listing support within the network to make sure that those voice calls always take place in a such of 911 voice calls.

393 Black listing is an approach to mitigate, limit or block some form of communication across the network. It's not quite the opposite, but a very different approach to handling traffic across the internet. Very often we construe the security practices, blocking malicious traffic, blocking traffic that -- there is a lot of work actually right now internal service approaches, how do we block attacks that are trying to impact or impair resource or user experiences across the network.

394 One of the considerations when we think about controls or ways to allow a network to perform some sort of value, we typically see three things that a network can do to differentiate or deliver value.

395 The first thing we see is virtualization. How does a network virtualize itself or across the common public infrastructure offer private domains for different users or businesses.

396 The second way we see a network that can differentiate itself is via an experience where much of the conversation has been today, how do we deliver a specific experience for an application or specific experience for a user.

397 The third way that we see a network differentiating itself is via security, how does it provide differentiating levels of security. It's actually the top right corner of my little slides where is the picture that depicts that.

398 So, those -- we think there are interesting ways to look at how networks can innovate and deliver value, So, again virtualization experience and security are all components of what a network can do to deliver value in the context of light listing or black listing for customers on that network.

399 Now, if we look at some of the tools, traffic management tools, that we see that are available. We'll talk about three, at least in our introduction here.

400 The first tool that we see available is what we typically call the "network level processing controls". Normal

controls that occur at the network level, many of which, as have already been spoken about this morning in terms of just serve or scheduling prioritization or shaping, how we control actual packets or flows going across the network.

401 Historically, these types of controls have been what I would term to be static in nature. We determine what they should be in advance, much the same way that we determine how traffic lights should work and they don't very necessarily base on load or capacity or what's happening in the network at the moment. Very useful, but sometimes limited in the approach that they can do when used in isolation or used just by themselves.

402 The second traffic management tool that we spent time talking about this morning is what we will term application processing controls or deep packet inspection or DPI.

403 This is an approach that is more dynamic, it watches what's happening on the network and it can make decisions based on what it sees at its point in the network and can take action real-time based on what's happening, whether that be on a specific application, for a specific type of attack, for a specific amount of capacity or bandwidth being utilized, but the network basically becomes more dynamic in this capacity and can react to something that deviates from the static model that we may have envisioned originally.

404 Now, deep packet inspection can be used in conjunction with the network processing controls that I spoke of earlier and can be used to trigger those and make them more dynamic in nature as well.

405 Now, the third type of traffic management tool that I will speak to we call policy management processing controls. Not to be confused with regulatory policy, but policy management is the act of -- it's similar to DPI in that it can become dynamic in nature. But we can have a function within the network that can broker or interact between users or between applications, or between networks for that matter, to differentiate how the network behaves, to blacklist or whitelist what's occurring in the network based on specific requests or specific demands in the moment.

406 Policy management can be used in conjunction with deep packet inspection and can also be used in conjunction with the network level processing controls.

407 So DPI and policy management are tools that we can leverage to help innovate at the network level to react real-time to concerns or expectations that may occur in the network and give some flexibility in what we might do in the network.

408 So looking at those tools, we feel that it's very important that innovation is able to occur at the network level and how we differentiate and control the flows that go across the network.

409 If you look at how any sort of interaction occurs across an IP network there are typically three constituents that are involved with how that works. There is the source of the application, there is the network itself for delivery, and there is the consumer of the application.

410 Using tools such as DPI or policy infrastructures can give us the ability to actually allow those to coordinate where the application or the user can actually coordinate a network.

411 Feedback can exist between what have historically been independent domains that don't know anything about each other. It gives us some flexibility and some capabilities to continue to innovate and build new levels of service and new offerings moving forward and not be stuck in a world where an application exists in a silo completely independent of the networks that it runs across, completely independent of the customers that access that network.

412 So having the ability to actively interact, to provide feedback loops, if you will, to control user experience, to control virtualization or to control security provides interesting levels of flexibility that we believe will allow the network to innovate, to keep up with innovation that's occurring in the application's base today.

413 I think there is a wonderful amount of innovation occurring actually at all three areas.

414 On the application side there is huge amounts of R&D and innovation occurring in things such as as simple as cloud compute where an application can scale how it is delivered to a user based on concurrency. A more popular application gets more access to more processing and access to more memory to deliver its application to users.

415 Having a network that can understand that those applications are becoming more interesting or more valuable to their customers and to react accordingly with a cloud compute framework is an interesting capability, is an interesting offer. It's a nice way to innovate to multiple different parts of the network at the same time, the application areas, the network areas and the user areas.

416 So, in summary, we find if we look in general at Internet traffic management philosophy, having the ability to innovate, having the ability for networks and applications to innovate together on behalf of and in conjunction with those users we think is very key moving forward.

417 And if we look at the kinds of applications that occur on the network today versus if we look back 15 years ago the majority of the Internet was simply a little bit of Web, mostly file transfer, and some e-mail. The types of applications that we leverage today are fundamentally different than how we built these networks originally.

418 If I look back 10 years ago, if I had an ethernet connection for my laptop I had a 10 Mb or 100 Mb connection, my laptop was very -- it statistically multiplexed well together with Doug's laptop next to me and so normally I would send out for e-mail or I would send packets or receive packets from the Web and then my PC would sit quietly. And then Doug's PC would perhaps do the same sorts of requests and we could coordinate and sit side-by-side very effectively.

419 Many of the new applications and the really innovative and valuable things that we see happening across IP today behave very, very differently. Voice over IP, gaming, video traffic, they all hum, as I like to say. They don't talk and be quiet, they hum constantly and that changes fundamentally the effect that it has on a network, the affect obviously that it has within a data centre or on the server side for application delivery and how it is

delivered to the customer.

420 We think it's important that the networks and the applications are allowed to innovate together so that they can best take care of the concerns of those who are accessing those applications.

421 That concludes my formal opening statements. Thank you very much.

422 THE CHAIRPERSON: Thank you for your presentation.

423 You talk about whitelisting and blacklisting, that's not a binary choice. You can have both at the same time, can't you?

424 MR. STEVENS: Absolutely. Yes, sir.

425 THE CHAIRPERSON: Yes.

426 And then the three types of management tools that you're talking about, network level, policy management and application processing, if I understand you correctly network level is really basically what we just dealt with in the Bell application, right, the Bell and CAIP where we talked about throttling and slowing down part of the network or some users of the network at given peak hours in order to make sure that they don't impair the use of others.

427 The other one, the more dynamic one, the application of processing controls, when I asked Sandvine before you -- and maybe I misunderstood them so you, as a fellow expert, you tell me, but it seems to me they are saying that's where the future is, they are working on it, but actually they are not there yet. You don't have these dynamic controls that you can go deal with the congestion point or the problem point, both in terms of technology, in terms of economics, in terms of billing systems, in terms of user education. Those are the four categories. That still leaves a lot of work to be done before we get there.

428 Is that your view, too?

429 MR. STEVENS: Let me try to answer the question a slightly different way perhaps, to give a different view.

430 Congestion is challenging in that it needs to be dealt with where it occurs in the network.

431 Congestion, as I look at congestion typically it can occur in an access network, which is different than dealing with congestion that occurs in the core of a network further away from the customer. It can also occur at pairing points, where one network connects to another network or where one network connects to an application domain. So dealing with congestion can be challenging in that you have to determine where it is first and then how to react to it appropriately.

432 So typically we focus on congestion, and historically we focused on congestion at the weakest link. If I go back 10 years, the biggest problem for congestion occurred at pairing points where networks connected to each other. Frankly, that was the genesis for companies like Akamai and other content delivery networks to become valuable because they were able to bypass many of those pairing points to allow applications to get to consumers more easily.

433 So depending on where congestion may occur, and that can vary greatly from network to network -- in one network congestion may occur in the access network based on architecture or based on how it was designed, in another network congestion may occur at the core of the network or in multiple places at once.

434 So a holistic strategy to deal with congestion I think is challenged by understanding exactly where that congestion is and then how best to mitigate it or deal with it at that point.

435 THE CHAIRPERSON: But the underlying objectives that you try to achieve would be the same regardless of where that congestion occurs?

436 MR. STEVENS: Yes, sir.

437 THE CHAIRPERSON: Okay.

438 Candice...?

439 COMMISSIONER MOLNAR: Thank you and welcome here this morning.

440 MR. STEVENS: Thank you.

441 COMMISSIONER MOLNAR: I want to just follow up on your approaches here to traffic management.

442 MR. STEVENS: Yes...?

443 COMMISSIONER MOLNAR: You put in your presentation two methodologies, whitelisting and blacklisting, and in your submission you noted that there were three approaches, the third being the consumption model. That I understand would be bit caps and different user consumption limits.

444 You didn't mention that here today. What are your thoughts on the consumption model as a means of managing traffic?

445 MR. STEVENS: I apologize for not having it in my formal presentation today as well as what we wrote. My rationale for doing that is whitelisting and blacklisting are typically more dynamic reactive approaches to dealing with the challenge in the moment.

446 Consumption models are useful and have been used in many parts of the world to deal with the challenge of the 5 percent user. Typically in most networks 5 percent of the customers consume somewhere between 1/3 to 1/2 of the resources of the network and so different consumption-based models can help deal with those heavy users and mitigate the amount of traffic that they put on the network.

447 However, as one of the analogies or one of the stories that was used already this morning, Michael Jackson dying still doesn't mitigate the fact that congestion will occur. I experienced it personally. There was news stories I was trying to get access to that I couldn't because actually -- the network was congested, but I actually think that the application servers were congested as well so I was getting failures trying to just simply launch webpages.

448 So the consumption model doesn't help in the challenge of something unexpected happening in the world and having to deal with that in real time.

449 I think it does help in the general trend of a small number of people impacting a great number of people in

more of the steady state.

450 As Sandvine talked about this morning, if we look at general traffic modelling we can find the peaks and knowing where the peaks are on a given Monday through Sunday and what times of day the peaks occur in a specific network, we can help engineer that network appropriately for those peaks.

451 And a consumption-based model can help us -- having a consumption-based model helps us in that steady state definition of how we manage our network and in most cases would mitigate the size of many of those peaks based on those heavy users not using as much traffic. Interestingly, many of the heavy users are completely unaware that they are heavy users.

452 Whereas whitelisting and blacklisting are much more real-time in nature, which is why I spent the time to present them today. They can deal with congestion challenges regardless of where they occur or how they occur.

453 COMMISSIONER MOLNAR: As someone whose background was in telecom I mean essentially the consumption model was the method of managing peak period traffic or in large part, right, we had time of day pricing and peak period and off-peak period pricing that was intended to manage consumption.

454 MR. STEVENS: Yes.

455 COMMISSIONER MOLNAR: You speak of it being for the 5 or 10 percent, the heavy users. But can't it be used more effectively to manage all traffic on the network?

456 MR. STEVENS: Actually I will go back to something that Sandvine said earlier.

457 I think part of the challenge here is there is a user understanding of how IP works and there is no current understanding -- on my cell phone I understand that a voice call during the day will cost me more than a call at night, but on IP I don't have that current understanding.

458 So perhaps economic-driven models, consumption-based models, time-of-day based models could move those peaks around and help us in the steady state, absolutely. Again, in the steady-state.

459 I think one of the challenges we are still left to deal with is an unintended incident that causes us to deviate from the steady state. You know, in the phone network we used to call it the Mother's Day event. I could never call my mom on Mother's Day because everybody was trying to call their -- well, I don't know why there was never a Father's Day event, but there is a Mother's Day event and those types of problems occurring dynamically, unintended, you know.

460 If something like a Hulu suddenly released a video distribution to PCs -- which we have in the U.S. -- suddenly released in Canada, that could fundamentally change, then, with models and peaks overnight where consumption-based models may or may not have the same amount of effect on that.

461 COMMISSIONER MOLNAR: Okay, thanks.

462 I'm going to get back to that, because my understanding of the technologies such as DPI that are employed today are in fact dealing more with the steady state than with the death of Michael Jackson, with those, you know, unanticipated events. It's being used today to deal with anticipated steady state, you know, the peer-to-peer, as I understand, on an ongoing basis between 4:00 and 2:00, 4:00 p.m. to 2:00 p.m. That is steady state.

463 MR. STEVENS: Yes.

464 COMMISSIONER MOLNAR: So as I understand today, the applications are not being used dynamically to deal with unanticipated loads on the network, they are being used to manage the ongoing load of the network.

465 But we can get back to that maybe a bit later.

466 I want to talk a little bit -- ensure I understand these concepts of blacklisting and whitelisting.

467 MR. STEVENS: Okay.

468 COMMISSIONER MOLNAR: you mentioned you can use the two together.

469 MR. STEVENS: Yes.

470 COMMISSIONER MOLNAR: Blacklisting -- they are both application or service-specific.

471 Is that correct?

472 MR. STEVENS: Or they could be user-specific.

473 COMMISSIONER MOLNAR: Or user-specific?

474 MR. STEVENS: It depends on -- again, the technology gives us options, how we choose to leverage them would be different for that.

475 COMMISSIONER MOLNAR: Okay.

476 In your submission you spoke of whitelisting within a walled garden and within what you termed an open garden.

477 MR. STEVENS: Yes.

478 COMMISSIONER MOLNAR: I want to ensure that I understand those concepts.

479 The walled garden, is that -- does the walled garden touch the public Internet or -- I'm thinking of something like an IPTV application.

480 Are there applications within a walled garden that connected to the public Internet?

481 MR. STEVENS: Typically not.

482 Typically a walled garden is restricted to an IPTV or perhaps a voice over IP services that replaces the PSTN, so they are normally locally significant. They may share access to some of the same resources in the network. The physical connection that goes to my home may have a subset of it that is used for IPTV and another subset that's used for IPTV and another subset that's used for Internet.

483 COMMISSIONER MOLNAR: Yes.

484 MR. STEVENS: So there may be an overlapping of physical resources.

485 But yes, there wouldn't be -- I wouldn't gain access to the walled garden content someplace else.

486 COMMISSIONER MOLNAR: So the open garden would have access to applications over the public Internet.

487 Is that correct?

488 MR. STEVENS: Typically, open garden -- as we have defined that, and that's a phrase that we have defined -- is actually public Internet applications that have the ability to interact with a network to get a service from the network that they need to be useful to their customer.

489 An example I might use, right after 9/11 I watched a lot of news for about two or three months. It was the same news every day, but I watched a lot of news. And one of the ways I got news was I subscribed to RealNetworks Super Pass, which had a streaming news service I could get 24/7 on my PC.

490 And it worked pretty well during the day and I could watch the news on a screen on my PC while I was doing my work. But from about 6:00 to 11:00 at night and my home it didn't work at all. It would stream for about 20 seconds, then it would stop, and it would stream for 10 seconds and then it would stop and rebuffer. There was congestion on my network to my home in the evenings and so the application itself was very, very poor and I stopped my subscription to RealNetworks because the experience I received for it during the evenings was very bad.

491 So today as we would look at that, that is normally termed an over-the-top application. It's just some Internet application that has access to me and I get it as best effort.

492 And for many applications best effort is sufficient. In the case of streaming news, it's not sufficient. Best effort, if there is no congestion it's fine, but if there is congestion then it's a pretty unusable application for me.

493 So we would term an open garden as the ability to expose publicly the capabilities of the network that carrier might only have for their walled garden and to allow something like a RealNetworks to be able to get -- if I so desired, to be able to get RealNetworks in a way that was more appropriate for the application itself than just best effort.

494 Does that make sense?

495 COMMISSIONER MOLNAR: I think it makes sense. I think I understand what you said.

--- Laughter

496 MR. STEVENS: Okay.

497 COMMISSIONER MOLNAR: But I'm having some difficulty in understanding in an open garden concept whitelisting obviously preference is given, priority is given to certain applications.

498 MR. STEVENS: Yes.

499 COMMISSIONER MOLNAR: So who is it that decides on that priority?

500 MR. STEVENS: It would typically be me, the consumer. I would decide that that was important to me and I would work -- there would be signalling either from me directly to a policy server or on my behalf from the application to the policy server, which is why I show the little arrows on the drawing.

501 So that on my behalf the application could tell the policy server that I am watching video right now and to prioritize that. Or I could tell the policy server that I'm watching video right now and to prioritize that.

502 COMMISSIONER MOLNAR: But in a period of congestion when everybody's doing something --

503 MR. STEVENS: Yes...?

504 COMMISSIONER MOLNAR: -- how does whitelisting work?

505 I'm trying to understand. If you say it's the consumer, I mean the consumer is doing one application and my neighbour is doing another one --

506 MR. STEVENS: Yes.

507 COMMISSIONER MOLNAR: -- and Commissioner Katz is gaming.

508 MR. STEVENS: Yes. I will use gaming analogies.

509 COMMISSIONER KATZ: Just stay away from porn, eh!

--- Laughter

510 MR. STEVENS: I will make sure I use gaming analogies for the rest of my stories here.

511 COMMISSIONER MOLNAR: So I'm just trying to understand in the notion of whitelisting --

512 MR. STEVENS: Yes...?

513 COMMISSIONER MOLNAR: -- where there is priority given --

514 MR. STEVENS: Yes...?

515 COMMISSIONER MOLNAR: -- in periods of congestion, who is deciding this priority?

516 MR. STEVENS: Again, I guess from a consumer's perspective I would be deciding that a specific application is more interesting to me.

517 I think if I go back to a question that was asked earlier about minimum guarantees to a customer, could I assure minimum guarantees. If I look at that question ubiquitously, to guarantee a minimum amount of bandwidth to a particular home is pretty close to impossible to do at all times, but I can work to get minimum guarantees for a specific application for a period of time.

518 I can solve the simple problem where I know the endpoints, I can't find the infinite problem where I don't know all the places where I might be going to get access to information.

519 So I think this is an implementation of a specific minimum guarantee that I could get on my behalf and I would choose to leverage it, perhaps in the case of my example, for watching news from RealNetworks or perhaps to play games on my Xbox.

520 Does that help?

521 COMMISSIONER MOLNAR: I'm sorry, I'm having more trouble with this than I should perhaps.

522 MR. STEVENS: Okay,

523 COMMISSIONER MOLNAR: But I'm trying to understand in a period of congestion, when everybody is seeking to access the network for their preferred application --

524 MR. STEVENS: Yes...?

525 COMMISSIONER MOLNAR: -- how does whitelisting work to choose amongst that group of users or it doesn't?

526 MR. STEVENS: Well, it could create priority in the network and so in times of congestion the traffic that I asked to be prioritized would do better than traffic that wasn't, that I didn't ask to be prioritized.

527 So if my son was playing games at the same time that I'm trying to watch my news, his traffic wouldn't fare as well during congestion as my news would, because I would ask for that to be prioritized ahead of his gaming traffic. So it gives me the ability to determine what I think is more important for my home and what I want to do.

528 COMMISSIONER MOLNAR: So this technology exists today?

529 MR. STEVENS: It does.

530 COMMISSIONER MOLNAR: I know that I personally have never made any choices as to what are the priorities within the traffic from my home.

531 MR. STEVENS: It does exist. It's not necessarily widely deployed in Canada. There are deployments in other parts of the world where it's more widely deployed to allow users to make those types of determinations or to say that a specific application -- I would like to sign up for a specific application to be delivered to me in a certain way. So those exist in different places of the world.

532 So the technology is there, it's not as widely deployed.

533 COMMISSIONER MOLNAR: And this is different technology than the technology we have heard? DPI is obviously a technology we have heard a lot about in this proceeding.

534 MR. STEVENS: DPI can be part of that solution.

535 In my experience, Juniper is -- we have DPI technologies within our portfolio, we also have policy management technologies, as I spoke to. So in my experience my answer would deviate towards the policy management framework as the technologies that would allow this to happen more than the DPI, but both -- again, they can typically work in conjunction with each other to deliver these services. You have flexible models available.

536 COMMISSIONER MOLNAR: Is it common that where whitelisting is being used today that it is at the consumer -- it is at the end consumer that the priorities are being chosen or is there also applications where priorities are being determined by the service provider?

537 MR. STEVENS: I think, if I look at the conversation of whitelisting generically, there are cases of service providers who have decided to prioritize one sort of traffic ahead of another. A service provider may decide that Voice over IP traffic is more important than internet traffic, and they have decided that for all of their consumers.

538 So they will engineer their network to treat Voice over IP traffic differently than other traffic.

539 Generically, whitelisting meaning biasing the network to behave, preferably, for one sort of application or user than another, there are cases when service providers have decided, usually publicly, to my knowledge, what application is prioritized ahead of another.

540 Leveraging technologies such as Policy allow that to be more dynamic in nature, where I can change it as real-time, versus a service provider simply saying: Voice over IP is more important across my network. I will make sure that that gets through first in times of congestion.

541 That is a rather static model versus a more dynamic model.

542 I might say for my home that Voice over IP isn't more important. Maybe video or gaming is more important. I can have that flexibility in what I want to do.

543 COMMISSIONER MOLNAR: I understand that, in your view, whitelisting is preferred over blacklisting as a means of managing congestion.

544 MR. STEVENS: I think they are both innovative tools that are necessary.

545 We tend to spend more time talking about whitelisting for the perceived value that it can deliver to those who have expectations of specific quality.

546 As we heard earlier this morning, the conversation of user expectation, or how do we assess the quality of the connection that we have, is typically very application-dependent.

547 I could lose 90 percent of my packets going from my e-mail, and I would have no idea that there was so much congestion for my e-mail.

548 But if that happened for my video, as it did -- actually, I think I only lost 10 or 15 percent of the packets for that. It made it unacceptable.

549 Assessment of value varies greatly by the application that we are accessing at the moment.

550 Whitelisting is interesting in that it allows me to determine which applications I am assessing value on.

551 Blacklisting is useful in multiple contexts, but in the case of congestion, to mitigate the aggregate congestion, so that everything works a little bit better and gives me an average better experience for all applications.

552 My video still may not be as good as I want it to be, but it would be better than it would otherwise be.

553 It's not two sides of a coin. We can take different approaches. But my view, and why I spend more time talking about whitelisting, is that I like the ability to make the decision of what is important to me, and how can I have the network behave in a way that is useful, for what I deem to be useful.

554 COMMISSIONER MOLNAR: There are two sides to the coin, as you kind of mentioned. Can either one be effective on its own in addressing congestion, traffic-based congestion on the network?

555 MR. STEVENS: In the long-term, I don't think so. I think that both are very --

556 Again, we don't know even what is going to occur next month, when we are talking about IP and the applications that are out there.

557 So having the ability to deal with congestion ubiquitously, just simply deal with the act of congestion and what is happening in the network, is useful.

558 And having the ability to determine what I find to be more important than something else is also useful.

559 So I think they are two important tools that give us the flexibility to innovate at the network layer to make things better for our customers.

560 COMMISSIONER MOLNAR: I would like to speak about the technologies that you presented here today and have discussed in your submission.

561 You mentioned three different types of technologies: packet processing, DPI, and Policy and Control technologies.

562 I understand, as well, from your submission, that you provide all three of these technologies today.

563 MR. STEVENS: Yes.

564 COMMISSIONER MOLNAR: In order to effectively manage traffic, can any one of those technologies manage traffic, or is it a combination of different technologies together that manages traffic?

565 MR. STEVENS: It is typically a combination, and we are seeing more of that moving forward than we did in the past.

566 If I look back in time, typically it was just the packet processing or the network level controls that we leveraged, in more of a static constraint. We engineered our networks, and we expected them to behave a certain way. What that didn't do is deal with unintended peaks, or deal with, you know, flash mobs and everything else that we talked about this morning.

567 What DPI and Policy provide for us is this dynamic nature, and often networks use them, in conjunction with the packet processing or the network level controls, to make those more dynamic in nature, to change queuing or shaping or Div serve or MPLS interaction dynamically, versus having just one static model that we built in advance and hope that it stays appropriate.

568 COMMISSIONER MOLNAR: Your Policy and Control technologies, you mentioned that they are not used in Canada today.

569 MR. STEVENS: I mentioned that they weren't used to allow a user to make selections of what they think is more appropriate.

570 We do have Policy and Control products deployed within Canada in different uses.

571 COMMISSIONER MOLNAR: And where they are deployed today, it is the service provider who is setting the policy rules, establishing priorities and so on?

572 MR. STEVENS: They are actually not -- I am talking about the policy management functions that we offer in the context of dynamically changing how a network behaves.

573 Our Policy service can do many things. As they are deployed in Canada today, they are being used not to do prioritization, or not to be doing anything in the context of whitelisting or blacklisting, they are actually being used to manage authorization onto a network.

574 There are multiple things they can do; I was trying to keep my answer in the context of the interests of this hearing.

575 COMMISSIONER MOLNAR: Okay. Now, I am just trying to understand, because having the ability for the consumer to set the priorities, and the consumer can change those dynamically, and that, somehow, would be sufficient to address congestion management on the network is an interesting -- you know, clearly, then, there is little potential to be discriminatory, if every consumer is getting what they desire.

576 But that's not available in Canada.

577 MR. STEVENS: The technologies are available; it's not deployed.

578 COMMISSIONER MOLNAR: Right, it's not deployed --

579 MR. STEVENS: But I also want to be careful. I don't want to paint a policy framework and the ability to determine what I think is important as a panacea.

580 I think that we do need to have flexible and innovative strategies in place.

581 Even if I determined that the video news that I wanted to watch was the most important thing, and perhaps Voice over IP was the second most important, my children may have a really bad gaming experience if there is a lot of congestion occurring, and that would still make me dissatisfied.

582 Obviously, I can't prioritize everything that I do. I have to make decisions on what I think is more valuable to me and less valuable to me.

583 But part of the value of the internet is the access to many different, disparate things, and many of those actually have a very low expectation of experience. Best effort is completely sufficient for many things that we do.

584 But best effort in a very highly congested environment is still pretty challenging, so I do think that we have to have the flexibility to have multiple different strategies in place, and I think that the ability to whitelist is one of those that is very intriguing and of great value, I think, to the consumer.

585 COMMISSIONER MOLNAR: But it will not, on its own, address the issue of congestion.

586 MR. STEVENS: I don't think it's that easy, unfortunately.

587 COMMISSIONER MOLNAR: I think you are likely correct.

--- Laughter

588 COMMISSIONER MOLNAR: If video becomes as popular as everybody predicts, and everybody ticks it off as their priority, I am not quite sure where we would get --

589 MR. STEVENS: Yes.

590 COMMISSIONER MOLNAR: So, in that case, you are back to blacklisting?

591 MR. STEVENS: You still have congestion to deal with, and having effective ways to deal with congestion.

592 I was actually trying to download a YouTube video to show my mother this weekend, and it took a while. I sit on a 6 megabyte connection, so...

593 Congestion occurs at many places, and how I deal with that would be -- again, dealing with congestion by itself has value to the ubiquity of things that we want to do. Whitelisting has value in the specific things that I care

about.

594 COMMISSIONER MOLNAR: Okay. The approaches to traffic management, are they different depending on the technologies that are deployed in the ISP network?

595 Would you use the same approaches in a mobile network, a satellite network and a cableco network, for example?

596 MR. STEVENS: If we look generically at IP, the concerns are basically the concerns. Congestion is definitely a challenge, and how we deal with congestion is a problem.

597 At the core of those networks, they are all fundamentally the same -- the core of a mobile, versus a fixed line, versus business, versus residential.

598 Away from the consumers, at the core of the IP network, the concerns are basically the same concerns, and how we deal with them would be roughly the same.

599 In the access networks, that's where the technologies vary. The concerns are still the same; the technologies leveraged might be a little bit different.

600 COMMISSIONER MOLNAR: The technologies that you provide, are they used on all networks?

601 MR. STEVENS: They can be, yes.

602 COMMISSIONER MOLNAR: They can be?

603 MR. STEVENS: Yes.

604 COMMISSIONER MOLNAR: I would like to focus for a minute on deep-packet inspection, first of all, as it relates to DPI.

605 Many of the practices speak about application-specific activity using DPI, peer-to-peer being the obvious application that has been discussed a lot in this proceeding.

606 MR. STEVENS: Certainly.

607 COMMISSIONER MOLNAR: Are there other ways that DPI can be used to manage traffic?

608 MR. STEVENS: We leverage DPI technologies extensively for security purposes: How do we protect resources from coming under attack.

609 I think that DPI can be used in lots of different ways. It's the ability to understand more than just the destination, the IP address of a packet, and based on that understanding, be able to perform actions.

610 If you look at our product line and our entire next generation of firewalls, they are based very heavily on DPI technologies, and being able to determine what flows are happening in the network, and to make decisions to protect the resources based on that, as well.

611 So I think, again, DPI in and of itself is a relatively broad technology conversation. We've been talking about it in the terms of perhaps mitigating peer-to-peer. You know, I would talk about it a lot in the context of protecting against malicious service attacks or other sorts of security concerns.

612 COMMISSIONER MOLNAR: M'hmm. You actually used the term in your submission that DPI is used to sniff out traffic flows in order to take action.

613 MR. STEVENS: M'hmm. That's a pretty technical phrasing I think.

614 COMMISSIONER MOLNAR: Yes. Is there any kind of limit on how a traffic flow is defined? What do you mean by a traffic flow?

615 MR. STEVENS: Our technology typically looks for signatures, looks to understand a specific type of traffic, whether it be -- does it conform to the proper framing for a video flow or a voice flow or things like that.

616 We don't -- we definitely don't look at payload or anything like that. Our focus is to understand, are the protocols themselves being properly leveraged or properly used. As many malicious intents look good but are leveraged -- they leverage the packets improperly.

617 COMMISSIONER MOLNAR: So, can you define a traffic flow by customer?

618 MR. STEVENS: Depending on how the network is architected, I could -- you know, I've got technology that can look on a per customer basis and determine -- and depending where they're at and network address translation, there's several concerns in the network but, yes, I can look at flows on a per customer basis.

619 COMMISSIONER MOLNAR: Or a class of customer, retail versus wholesale, for example?

620 MR. STEVENS: That would typically -- one way that would be done is by range of addresses, but yes, you could look at classes if need be.

621 COMMISSIONER MOLNAR: So, with DPI you're not really limited as to how you define a flow, you could define it as an application, as a customer.

622 Can you define all traffic flows by a time of day?

623 MR. STEVENS: Well, I would just --

624 COMMISSIONER MOLNAR: You wouldn't need to, I guess.

625 MR. STEVENS: Because it's the time of day. I could change how it behaved based on time of day.

626 COMMISSIONER MOLNAR: Okay.

627 MR. STEVENS: And I could do that, you know, those -- I could change how the device behaves at different times of day, yes.

628 COMMISSIONER MOLNAR: Let me ask you, just so I understand, you provide a DPI solution and once that solution is in place in an ISP's network, is there cost differences to changing how you use that?

629 For example, if you began -- I mean, as I understand it, and this is what I'd like to understand from you.

630 MR. STEVENS: M'hmm, sure.

631 COMMISSIONER MOLNAR: If I've got this correctly, it's basically intelligence software, and so if I purchase the software I then program it to do what I want and when I want, so I could initially use DPI to take action on traffic at a certain time of day, I could -- then if I chose to, could I program it to identify certain customers and take action on those customers, or use it more dynamically just by changing how I program the set of policy rules

that it's taking activity on?

632 MR. STEVENS: I may not be the best vendor to answer that question. Our DPI isn't that flexible.

633 COMMISSIONER MOLNAR: Oh.

634 MR. STEVENS: Being more focused on threats than it is just generically on processing everything within a network.

635 So, that may or may not be possible based on vendor-by-vendor implementations. Ours isn't quite that flexible, so...

636 COMMISSIONER MOLNAR: Okay. Would you be able to comment on using DPI to throttle peer-to-peer traffic in the upstream versus downstream; does it make any difference? Are there different requirements to throttle in both upstream and downstream?

637 MR. STEVENS: Again, I may not be the best vendor to answer that. Fundamentally dealing with congestion is dealing with congestion and there -- upstream versus downstream in different network topologies will have different thresholds for congestion and, so, dealing with congestion in different places can vary in how you want to react to that.

638 COMMISSIONER MOLNAR: Okay.

639 MR. STEVENS: But I think the technology would be roughly the same in all cases.

640 COMMISSIONER MOLNAR: Thank you.

641 I just have a couple of questions related to privacy.

642 MR. STEVENS: M'hmm.

643 COMMISSIONER MOLNAR: And using DPI to sniff out traffic flows or drill down to see what end customers are using.

644 For what information -- actually on page 15 you say that you can drill down to see what end customers are using the applications and the amount consumed.

645 What would be the purpose of monitoring and collecting this information?

646 MR. STEVENS: Actually typically our phrase in there I believe is to look at billing and SLA concerns and, so, if you have an SLA from me for voice over IP and I need to monitor then how much of that voice over IP traffic got through the network so that I can verify that I actually delivered on that SLA.

647 And, so, there are cases when, you know, it's very important to understand how much of a specific type of traffic got through the network so that I can guarantee that I actually delivered as promised.

648 COMMISSIONER MOLNAR: Okay. So, other than quality of service and service level agreements, just for purposes of managing congestion, is there any reason for DPI to drill down to end customer information?

649 MR. STEVENS: I think it would depend on the policy that's being deployed by the carrier, and it -- you know, end customer information is a -- in the context of privacy gets kind of scary for me to start answering questions on, but if we're dealing with trying to threshold a specific high consuming customer, then I need to make sure that I'm taking the appropriate actions on the appropriate customer.

650 And, so, it is important that I have the flexibility to determine that Doug's children are the ones that consume all the band width, not mine, and the threshold that they're doing within the network during a given period of time, versus just thresholding all application types in that period of time, so I can take actions of a different type depending on the set of concerns that we have.

651 It doesn't mean that I profiled his children necessarily, but if congestion is being -- if congestion is being delivered by a small number of users, taking action on those number of users benefits everybody and doesn't impact anybody else at the same time.

652 Does that make -- we actually see implementations along this line in different parts of the world right now, where those users who are causing the greatest percentage of the congestion -- obviously the aggregate of everybody causes congestion -- but there are certain users who are causing a much greater percentage of that, action is taken to mitigate specific applications from them versus impacting everybody's applications at the same time.

653 So, you can -- and by the way, you can do those at the same time as well, just different options.

654 COMMISSIONER MOLNAR: Okay, thank you.

655 Those are my questions.

656 MR. STEVENS: Thanks.

657 THE CHAIRPERSON: Len?

658 COMMISSIONER KATZ: Thank you. I've just got two questions.

659 One is, one of the tools you identify here is something called policy management processing controls.

660 MR. STEVENS: M'hmm.

661 COMMISSIONER KATZ: Very interesting term. Is that a gracious way of saying service or application differentiation based on quality of service?

662 MR. STEVENS: Actually, policy management is actually a product category and, so, that's typically a software-based product that can interact with the user or interact with the application.

663 COMMISSIONER KATZ: For what purpose, to achieve what?

664 MR. STEVENS: Typically it's a white listing conversation to achieve some preferential treatment across the network. It can also be a black listing conversation if we're under attack. We also use Service Protection Architectures.

665 COMMISSIONER KATZ: So, it is differentiation of applications or users?

666 MR. STEVENS: Yes.

667 COMMISSIONER KATZ: Okay.

668 MR. STEVENS: It can be leveraged to do that and typically leverages the packet processing or the network

level controls and uses them dynamically.

669 COMMISSIONER KATZ: Do you believe consumer usage habits can be modified?

670 MR. STEVENS: In what context?

671 COMMISSIONER KATZ: Shifting -- how they use the network, when they use the network based on various tools or various economic as well as technical tools?

672 I mean, university crowds from what I gather, what I've heard in the past, is they download stuff when they go to class and they come back at night and they watch the movies or whatever.

673 There are some people who obviously have downloaded peak times in the evenings as well.

674 So, the question is, are there tools available that would allow for shifting of some of that non-real time downloading that would reduce the congestion in the networks?

675 MR. STEVENS: For steady state congestion, differing consumption-based models, economic models can be used to do that, to move download times to different periods of the day. Assuming that I don't have to wake up at one o'clock in the morning to start the download, I can schedule that in advance. So, there's some application dependencies with doing that.

676 But that doesn't necessarily deal with the concern of, you know, something happening that was unintended. So, again, more useful and steady state modelling and more efficient use of the capacity when my network is running at, you know, 15 percent utilization versus a hundred percent utilization.

677 COMMISSIONER KATZ: But, I mean, I've got grey hair now, so I can go back to the days when Mother's Day was the most congested day for phone calling on Sunday, and the networks went down.

678 MR. STEVENS: M'hmm.

679 COMMISSIONER KATZ: And there was nothing they could do to build enough capacity in those days because you knew that on that day everybody was calling their mom -- maybe they still are, I don't know, instead of e-mailing them -- but in those days the network wasn't built for that level of capacity, and so it happened, no different than the Michael Jackson death or anything else as well, these things are going to happen unfortunately.

680 MR. STEVENS: Well, I guess if we had seven Mother's Days that might have made that problem a little bit easier to deal with.

681 But, again, I think we can move people around to deal with what we anticipate or what we know is going to occur on a daily basis, but that doesn't help us with Mother's Day.

682 COMMISSIONER KATZ: Okay. Those are my questions.

683 THE CHAIRPERSON: Tim?

684 COMMISSIONER DENTON: Thank you, Mr. Chairman.

685 I guess my question may be the same to you as I have asked of many parties before us, and that is to link the useful information you're presenting to us with what our job is here as Commissioners.

686 Now, the job here is that we have a statute in the Telecommunications Act which says that:

"...except where the Commission approves otherwise..." (As read)

687 COMMISSIONER DENTON: The big out clause,
"...a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public." (As read)

688 COMMISSIONER DENTON: So, we're asked to frame a set of rules, if we can --

689 MR. STEVENS: M'hmm.

690 COMMISSIONER DENTON: -- to deal with the issues that you have so carefully explained.

691 So, I think that my point would be that if Juniper wishes to inform us further of, in final argument or however it presents its arguments, it would be very helpful to see the relationship between what you think we should be doing under section 36 and the information you're disclosing today, because in my mind I can't make instantaneously that leap between the two, our legal duty and the information you're presenting.

692 So, I think that's the thing I would say.

693 MR. STEVENS: Okay.

694 COMMISSIONER DENTON: Now, when you speak -- I just want to unpack a bit further what you were talking about when you were talking about interactivity between the applications and the network and innovating together.

695 That's a mighty huge concept, but could you just explain to us a bit further what you mean by that?

696 MR. STEVENS: If we look at -- there's a huge amount of innovation going on in the application space and there are very interesting and creative applications that are coming into existence that leverage IP and there are things that didn't exist conceptually even five years ago that we're trying to run across IP.

697 So, video across IP wasn't initially a goal, IP was a best effort medium, video doesn't work well on best effort unless I download it all in advance.

698 And so, real time -- the real-time aspect of many of the things that we're trying to do across IP networks today is based on interesting innovation going on in the application space.

699 We need to have similar innovation occurring I believe at the network layer to support that. I think allowing innovation to occur on one side and not on the other side is challenging in that the network is the medium upon which that application is delivered and if that medium is insufficient for the application, that stifles application creativity at the same time.

700 And, so, having the capability for -- well, historically applications and networks have been completely oblivious to each other, there's no care, no knowledge, no interaction, no ability for them to communicate.

701 If we look at the interesting innova -- one of the interesting innovations that occur in the application space today is in the construct of web services or service-oriented architectures.

702 Effectively what this does is it allows applications to talk to other applications. We couldn't do that just a few years ago, not effectively, not in an open standards-based way. We could do things, you know, in a proprietary

way between two companies that decided to work together, but not in a more open standards way.

703 We can leverage those sorts of frameworks to now allow applications and networks to talk to each other. Again, something that wasn't possible before this innovation occurred in the application side of the world.

704 And, so, I think it's important that we follow that trend of innovation and make sure that the innovation that occurs in the application space can be met by innovation that needs to occur in the network space to support it.

705 COMMISSIONER DENTON: Okay. Then I guess my only point would be is that when you give us your final advice on this --

706 MR. STEVENS: M'hmm.

707 COMMISSIONER DENTON: -- that there be a linkage between the very important things you're talking about with our statutory duty of not allowing for discrimination unless there's a reason to.

708 MR. STEVENS: M'hmm.

709 COMMISSIONER DENTON: And I think that linking your discourse, which is really quite important, to what we have to do so that either what we have to do doesn't mess up that, or that what you guys do is somewhat influenced by appropriate rules of non-discrimination.

710 End of message. Thank you.

711 MR. STEVENS: Absolutely. Thank you for that.

712 THE CHAIRPERSON: Suzanne, last question.

713 COMMISSIONER LAMARRE: Merci, monsieur le Président.

714 I'm going to ask you a question that I don't mean it to be unfair, I just want to understand the processes that you go through when you design equipment, and I understand that what your manufacturing corporation is aimed at providing equipment that will provide security to its clients which are, you know, Internet service providers.

715 And in answering a question from Commissioner Molnar regarding to what depth DPI inspection could do into getting information, you replied -- I'm not quoting you exactly -- but you replied that that will depend on the policy of your client.

716 So, going back to the fact that you're trying to satisfy your client, its policy, its business models and whatever because you have a business to run, and you have a research and development process --

717 MR. STEVENS: M'hmm.

718 COMMISSIONER LAMARRE: -- to provide for the equipment that your clients need. Within that research and development process, at what point do the privacy issues become a concern, the privacy of the end customers or the citizens that are at the end of the network from your client's infrastructure? Is it at the beginning, or is it just after the fact, or don't you just bother at all?

719 And I'm asking, I'm just trying to understand what factors in the solutions, the security solutions that you provide to your clients.

720 MR. STEVENS: I think -- the research and development that we do to protect our clients and to have deep packet inspection capabilities that can protect their resources is fundamentally focused on understanding what those threats can be, making sure that we can determine them, find them and then mitigate them.

721 Our focus isn't on, to my knowledge, any information or obtaining of any information that would have privacy concerns. You know, we're typically focused not on profiling subscribers, we're focused on protecting them from things that are coming toward them and making sure that those things are appropriate to not malicious.

722 COMMISSIONER LAMARRE: Okay. Thank you.

723 THE CHAIRPERSON: Okay. Thank you very much for your intervention.

724 We will take a very short break before we hear our last intervenor.

725 Thank you.

726 MR. STEVENS: Thank you.

--- Upon recessing at 1130

--- Upon resuming at 1135

727 THE CHAIRPERSON: Madame la Secrétaire, let's go. We are under time pressure.

728 THE SECRETARY: I would now invite PIAC, the Public Interest Advocacy Centre, on behalf of the Consumer Groups to make its presentation.

729 Appearing for the Consumer Groups is Mr. John Lawford. Please introduce your colleagues and you have then 15 minutes for your presentation.

PRESENTATION

730 MR. LAWFORD: Thank you.

731 Mr. Chair, Commissioners, CRTC staff and fellow parties to this proceeding, my name is John Lawford. I'm counsel with the Public Interest Advocacy Centre, here representing the Consumers' Association of Canada, the National Anti-Poverty Organization, which is now called Canada Without Poverty, and Option consommateurs.

732 We call ourselves the Consumer Groups and as we have done in many previous proceedings, we are pleased today to make oral comments on this proceeding. We are here today to represent the interests of Canadian consumers and in particular vulnerable consumers.

733 With me on the panel today are Dr. Barbary Cherry, Professor at the Indiana University Department of Telecommunications; Ms Janet Lo, who is our new counsel at PIAC; and joining us very shortly will be Alastair Warwick, who is a network consultant with Xinc IT.

734 We wanted to discuss the six questions posed by the Commission today. However, with the time constraints on the oral presentation, we have elected to concentrate on a few of them but we ask you to please ask us questions on the other matters if there is time in questioning.

735 The Commission needs to properly frame the inquiry in this proceeding and the conceptual approach taken in

this proceeding. Traffic management should be seen as the means to the end of ensuring open and equal access to the Internet for customers of Internet Service Providers.

736 The Commission has started well, with the goal of enabling customers to access the applications and services of their choice over the Internet. However, the Commission in its statement of the objective of this hearing appears to be balancing this goal with respect for the legitimate interests of ISPs to manage their networks.

737 We submit that where there is a conflict the Commission must prefer delivering that content to protecting the mechanism of delivery.

738 The Consumer Groups submit that this approach is required by the framework of common carriage which underlies the Telecommunications Act and the specific statutory sections at issue in this proceeding.

739 Section 36 protects content and transmission from interference by the carrier.

740 Subsection 27(2) prohibits unjust discrimination or any undue or unreasonable preference toward any person, including the carrier, in relation to the provision of a telecommunications service.

741 Both of these provisions of the Act are codifications of the common law wisdom that given the network operator's exclusive control over the delivery of the good -- which is here information -- in its possession during transmission, the law requires delivery of that information and content unaffected to the user of the network notwithstanding the convenience or the gain to the network provider in snooping or otherwise controlling the delivery based on what is being delivered.

742 The law also requires reasonably equal treatment to customers, competitors and others and just and reasonable pricing for comparable service.

743 This is just as a matter of public policy since the network operator is offering a service to the general public and making a profit from their public offering.

744 The network operator agrees to subordinate his interest to that of the customer in these two areas -- that is, non-interference with the message and non-discrimination amongst customers and others -- in exchange for the right to do business in this domain with the public.

745 This is the law under the Telecommunications Act. We note that despite the forbearance from regulation of Internet retail service, the Commission has retained authority under 27(2) and also to set future conditions of service under section 24, and that forbearance does not affect the Commission's continuing jurisdiction under and duty to apply section 36.

746 Before proceeding to the first questions, we are going to address the assumptions.

747 We are concerned that the Commission's second stated assumption, which is "Certain ITMPs, Internet Traffic Management Processes, may be appropriate for ISPs to use in order to maintain the integrity of their networks," could be interpreted as implicitly accepting that even prima facie violations of sections 27(2) or 36 could be valid if their purpose is protecting the integrity of the network.

748 There is no language in section 36 protecting network integrity and the intent of section 36 is to protect and ensure unchanged delivery of the customer's message.

749 The Commission's stated assumption could also stand on its head the process under 27(2) regarding unjust and undue discrimination on. Once a difference in treatment has been made out, the burden of showing that the discrimination or preference is not unjust or undue falls clearly on the carrier under subsection 27(4). This subsection requires factual evidence that is advanced by the carrier.

750 In this proceeding, the Internet Service Providers have not provided this clear and convincing evidence of network congestion requiring application-based throttling.

751 We invite the Commission's questions on 27(2) and on our view of unjust discrimination in relation to Internet traffic management practices and our expert Dr. Barbara Cherry is well positioned to outline the application of this common carriage obligation.

752 The burden is on the ISP to justify and to fully explain how deep packet inspection and throttling do not violate the common carriage rules expressed in section 36 and subsection 27(2). It is not for consumers to beg for reasonable traffic management procedures.

753 Secondly, the Commission assumes that section 7 policy objectives govern the circumstances under which the Commission will grant approval under section 36 for ITMPs. That is in the assumptions.

754 We are concerned that this exception under 36 will eat the rule. There is no easy way to reconcile the competing directions in the section 7 policy objectives. These objectives themselves do not provide a framework that respects the initial reverence of the common carriage principle of non-interference with the message expressed in section 36.

755 Section 7 objectives do not confer power and the discernable intent of section 36 is to minimize interference by carriers with the telecommunications they carry.

756 That is why we propose a different, three-part test for applications under section 36 to avoid it, which is nonetheless consistent with section 7 policy objectives and the Policy Direction and is more likely to elucidate the legislative intent behind both subsection 27(2) and section 36.

757 We will address the last question first, which is the framework under section 36 of the Act.

758 The appropriate analytical framework for the interpretation of section 36 in light of ISPs continuing use of DPI and other Internet traffic management practices is simply a matter of statutory interpretation and the Commission must get this interpretation right.

759 We have detailed our interpretation of Section 36 in our written comments and we refer you to them. However, in short, we say that section 36 has two separate clauses with two separate prohibitions: first, controlling content, and second, influencing the meaning or purpose of telecommunications.

760 We say, firstly, that editorial control is not the correct test for control under section 36 in these circumstances, and secondly, that section 36, in relation to Internet traffic, also requires the carrier to look no

deeper than the IP header.

761 The Consumer Groups therefore view all DPI-based Internet traffic management practices as prima facie violations of section 36. All ISPs that wish to use DPI-based ITMPs therefore should make individual applications under the Act.

762 This view means that even this proceeding should not be able to authorize a section 36 violation via DPI unless coupled with a formal application by an ISP to be exempted from section 36, with requisite proof filed and an opportunity for public comment.

763 Discussion of reasonable DPI-based ITMPs must therefore be considered only by the Commission under its section 36 jurisdiction to consider applications to avoid the strictures of section 36.

764 If applications under section 36 were made by the ISPs in this room today that have admitted to DPI-based ITMPs, not one of them would pass muster. None of these ISPs has revealed in sufficient detail exactly how they manage traffic below the IP header level at the packet level.

765 Bell and all of the other such ISPs have not answered the Commission's interrogatory question 8(c) on this and they have provided only vague descriptions of their ITMPs at the packet level. This is not good enough to win exemption from section 36. The Commission must know exactly what is affected in the transmission and how it is carried out if you are going to determine if a Canadian carrier is controlling content or influencing the meaning or purpose of telecommunications carried by it for the public.

766 The proper process under an application for Commission approval to carry on ITMPs despite section 36, we submit, is to place the burden of proof clearly upon the carrier to make out a serious problem by clear and convincing evidence and that there is a pressing need to address it, to require that any solution minimally impairs the network users' clear rights to access content and applications and use protocols of their choice, and that the proposed solution is in proportion to the harm sought to be controlled. If such approval is granted, consumers should be fully informed of the interference with their Internet service.

767 In our view, the Commission, in a standard procedure for all ISPs, could consolidate many such section 36 applications for the least contentious uses based on a list generated out of this proceeding. The Consumer Groups suggest that on this list could be ITMPs for spam control, spyware and other malware control and control of network attacks such as distributed denial of service attacks. Interference with the message might also be appropriate in certain defined emergency situations.

768 Criteria for less contentious applications could be uses that protect the end users from network-delivered content or telecommunications which are unsolicited and are manifestly harmful to a majority of network users or which seek to distribute life-saving emergency information.

769 After these mass applications the Commission could then invite each individual ISP to bring forward other DPI-based ITMP applications. These applications should be brought in a standard format, pass the previously mentioned test of necessity, minimal impairment of user rights and proportionality.

770 However, the Commission should assist ISPs by issuing guidelines indicating which applications would be more or less likely to be approved.

771 In the Consumer Groups' view, given the potential for abuse with interference with the message and discrimination on the part of those that use DPI-based ITMPs, the guidelines should favour applications that promote uses:

- 772 - that treat all competitors, users, applications and traffic equally;
- 773 - that do not increase rates to consumers for what is essentially similar service;
- 774 - that protect the privacy of users;
- 775 - that increase consumer protection;
- 776 - that increase security; and
- 777 - that facilitate emergency services.

778 It is instructive to contrast this proposed approach under section 36 with the present net neutrality debate in the United States.

779 In Canada, the Commission retains the authority to enforce common carriage obligations with regard to the provision of broadband Internet access services that the FCC currently does not. As described in Dr. Cherry's evidence, the Commission's retention of this common carriage authority is a significant advantage and that the FCC has unfortunately denied itself in addressing internet traffic management practices. The consumer groups urge the Commission to not forego on a defective basis what the FCC has given away on a DGRA-1.

780 And the momentum to reimpose common carriage type requirements in the U.S. is already intensifying. President Obama has clearly stated his support of net neutrality principles and as has the new Chairman of the FCC, Julius Genachowski.

781 Moreover, this past week, the NTIA and Department of Agriculture Rural Utility Service released a notice to funding availability calling for broadband initiatives and passing a broadband seamless legislation through Congress.

782 In the NOFA and under which 7.2 billion government appropriations will be awarded to expend broad band access to on certain and under-served communities across the U.S., the NTIA and the RUS specifically require broad band infrastructure applicants to commit to non-discrimination and inter-connection obligations and those are listed here, including adherence to BFCs Internet Policy Statement not to favour any lawful internet applications or contents over others, to display any network management policies in prominent location on the service provided web page and provide notice to customers the change of these policies and to offer inter-connection.

783 In addition, in a current broad band proceeding before the FCC required by Congress to develop a national broad band plan, consumer advocates are urging the FCC to reclassify high speed internet access as a

telecommunications or common carriage service.

784 In short, regulatory efforts with regard to neutrality in the United States are attempting to reproduce what the consumer groups contend are the basic requirements of common carriage in Telecommunications Act in Canada.

785 Turning now to Question 1. The consumer could see that the only acceptable uses of deep packet inspection and similarly invasive technologies as previously stated are those that protect end users from network delivery content that is unsolicited and manifestly harmful to a majority of network users.

786 Interference with the message might also be appropriate in certain defined emergency applications.

787 Totally unacceptable, therefore, is traffic management based on DPI where the goal is to ascertain what application or service the customer is using for the gain of the carrier. This would include targeted or behavioural advertising and price discrimination based on that knowledge.

788 So, what then are the criteria for identifying acceptable ones. Bell and the other DPI based ITMP-using ISPs should not be able to declare perpetual internet state of emergency when it lies in their power to build capacity to meet that demand.

789 This basic requirement is to adequately provision their network should do adequately provision their network, should inform any application for approval under Section 36 and the Commission should consider the following questions with relation to that.

790 Firstly: what are the alleged problems that the carrier asserts would justify an exception from Section 36?

791 Two: Has the carrier made the necessary or reasonable investments or other changes in practices that would obviate the need for an exception from Section 36?

792 And thirdly: given the problem, is the carrier solution proportionate to that, a solution to proportionate to that, given the importance of the unimpeded access of consumers?

793 And finally, we highly -- one practice that is very important to us and to consumers is that the Commission should enquire into during the application process, has the carrier made disclosures to customers that would provide them an opportunity to change their behaviour and eliminate or mitigate the alleged problems so as to obviate the need for or affect the scope of that exception?

794 In regard to disclosure, of course, Commission's Question 2. The previously mentioned consideration of how much disclosure the ISP has already made to its customers about its DPI or trawling practices is an X anti-obligation made under its application seeking exemption to Section 36 or an exposed disclosure requirement of DPI and trawling once these practices is approved is also key to customers and appears to be what the Commission is really addressing with this question.

795 And then the place for such exposed disclosure would be prominently on all ISP websites and this provision of a website linked to all electronic bills, on all electronic bills, excuse me, and that a minimum disclosure would state (1) exactly how trawling or similar traffic control is carried out and that's something that the companies, and that's the Bell companies, have so far refused to do, in confidence, even to the Commission thus far.

796 Secondly; the maximum average likely speed attainable for all affected protocols and applications during this trawling and, of course, you would identify which protocols you were reflecting when you made that statement.

797 The hours or days or other time periods when trawling is carried out, whether the ITMPS employed resulted in the collection of customers personal information or have the collection, the potential to collect that information, whether the ITMPS in any way affect the customer's billing and who would the company or customer may call to get further information about it and where to complain.

798 The consumer groups are also of the opinion that the wholesale service disclosure of trawling and DPI technology is necessary for those businesses to be able to inform their own retail and business customers of limitations on their service and who has imposed those limitations.

799 The consumer groups are also concerned that the ISPS claim confidentiality in certain aspects of DPI based traffic management. Due to the potential for privacy invasive marketing, based on profile, profiling made possible by DPI and other related technologies, that's a problem for us.

800 If ITMPS are truly for traffic management only, there should be little to no need for confidentiality limitations on the duty of disclosure to customers and in any case, the public interest should disclose and that such disclosure should weigh commercial interest.

801 The last major point I will deal with is privacy. The privacy aspects of DPI technology employed by all ISPS using these traffic management solutions are highly invasive of personal privacy of users.

802 The Heavy Reading report and then the submissions of many parties shows that DPI looks deep into packets of well below the IP header level, reveals what application is being used, which website visited or what other services used, the length of time of using that service, search strings and other information that reveals much detailed information about the internet behaviours of particular users.

803 Consumer groups view DPI as clearly violating the Telecommunications Policy goal of Sub-Section 7(i) which exhorts the Commission to protect the privacy of users. The Commission has repeated in the past that the Telecom Act allows a total carriage to a higher privacy standard than the Personal Information Protection and Electronic Documents Act.

804 So, we call the Commission to continue your interpretation of your jurisdiction this way.

805 THE SECRETARY: Mr. Lawford, your time is almost up. Can you conclude, please?

806 MR. LAWFORD: Yes. I'll finish this page and that will be it.

807 THE SECRETARY: Thank you.

808 MR. LAWFORD: Nonetheless, DPI invades privacy and fails even the Copeda(ph) test in three ways.

809 First; ISPS do not obtain informed consent to collect and use, and disclosure of this mostly sensitive

personal information.

- 810 Second; collection is not limited to the claimed use, which is just traffic management, but instead goes well beyond to gather information that is especially useful for marketing and potentially for price discrimination.
- 811 And third; ISPS in this proceeding generally do not make these collections, uses and disclosures clear to customers in contracts acceptable use policies and privacy policies and I'll conclude there.
- 812 THE CHAIRPERSON: Thank you for your intervention. I don't quite understand you.
- 813 You seem to think that DPI by itself is a violation of the Telecommunications Act, Privacy Act, but yet, on paragraph 31 where you talk which DPI should be considered totally unacceptable, you've said:
- 814 Therefore, totally unacceptable is a traffic management based on DPI where the goal is to ascertain what application or services in Canada the customer is using and here comes the key word, "for the gain of the carrier"?
- 815 MR. LAWFORD: Yes.
- 816 THE CHAIRPERSON: Yes. For the gain of the carrier, that part I understand, but I don't see if you take those off, if they don't use it for the gain of the carrier, but they use it to maintain the integrity of the network, what this is all about, they want to make sure that internet functions, that when you use the telephone... make a telephone call, you don't get latency when you play or see a movie, you don't get jitters, et cetera.
- 817 Why is the use of DPI for that purpose calling to you so contrary to the Telecommunications Act? I just don't understand it.
- 818 MR. LAWFORD: In terms of privacy violations, it doesn't matter if they use it for any particular purpose, they have still gone down and seen what I am doing on the network at that time.
- 819 So it can still be, as far as 7(i) is concerned, a problem.
- 820 Now, there are larger goals that you are talking about and that's part of the process that we are here to try to determine as how far they need to go in managing traffic below the IP level, in order to make their systems run.
- 821 What we are saying is that the way that the Telecom Act is structured, they have to come to you and give you as much evidence as they possibly can if they are not doing it in an unjust way and that they need to do it.
- 822 So, it's not for us, but for them to come and show these problems as they have to show the congestion and they have to be clear about it.
- 823 THE CHAIRPERSON: But don't you agree with me that the key is that the network could function as an integrity, you know, that if there is... if you say any diffuse of DPI is a violation of privacy, let's say from -- I don't think I accept that.
- 824 If it's not being used for anything except for maintaining the integrity of the network, not for marketing therefore, not for consumer research or anything like that, then clearly since it has different objectives and in that scenario is the integrity of the network has to come first because it's -- the network isn't then it's -- the users cannot use it and they don't get the benefit for which we set the Act up in the first place.
- 825 MR. LAWFORD: We have given some indication that -- in examples like spam and denial of service attacks, that's situations where the integrity of the network is under attack, and those are likely to be appropriate and approved.
- 826 THE CHAIRPERSON: That's Legislation. That's a totally different world. Parliament can do what they want. We are talking about us, here, interpreting the existing legislation.
- 827 MR. LAWFORD: Yes, yes and let me say under Section 36 you could allow uses like that because they are protecting, they are clearly protected in the use of the consumers and the integrity that then if you want to define it as what's useful to consumers.
- 828 THE CHAIRPERSON: But the Section 36, the usage that you envisage here, how do you reconcile that with the direction that we have to intervene as little as possible, you know, to basically set guidelines and have the networks operated to the maximum efficiency and step into it, for you really are talking here in X-anti regime where you cannot do anything to produce the integrity unless you get our prior approval, which is not as far as I understand to being directed by the Cabinet to interpret and apply the Telecommunications Act?
- 829 MR. LAWFORD: No. There are methods which are not DPI based, which you can presently use, DiffServ and other network management protocols that are already in place. There are bit caps, there is usage-based billing, there are lots of other ways to get to reducing congestion than to use DPI-based application-specific methods of getting there and, unfortunately, that seems to be the first choice rather than the other methods.
- 830 THE CHAIRPERSON: And you are against using DPI-based methods for what reason?
- 831 MR. LAWFORD: I'm sorry, I didn't hear the question.
- 832 THE CHAIRPERSON: And why are you so concerned about DPI-based methods if they are used purely to maintain the integrity of the network?
- 833 MR. LAWFORD: There will be uses of that which inevitably will go beyond just that. They will be --
- 834 THE CHAIRPERSON: So you are worried about abuse?
- 835 MR. LAWFORD: There will be abuse. There will be abuse of it for privacy violations, there will be price discrimination, there will be other forms of discrimination and innovation stifling that will go on, yes. That's our view.
- 836 THE CHAIRPERSON: Okay. Thank you.
- 837 DR. CHERRY: Commissioner --
- 838 THE CHAIRPERSON: Suzanne...?
- 839 DR. CHERRY: -- von Finckenstein, may I assist? I might be able to offer some comments that may assist in understanding the consumer group's position.
- 840 With regard to common carriage, common carriage is a very specific industry-specific form of regulation of centuries long standing that grew out of the common law and apply to certain kinds of businesses and in the 19th century, with industrial revolution and so forth, the common-law version was considered not adequately

enforceable because of the burden of proof that was put on the customer to complain, and there were all sorts of discriminations and abuses that grew out of it.

841 And in order to better enforce the basic obligations of a common carrier -- this is when we started having statutory forms of common carriage where we actually designated specific regulators to oversee the industry, an important component of which was switching the burden of proof under statutory form of common carriage in Canada, as well as the United States, the burden of proof is on the carrier to show that its practices are just and reasonable.

842 So one of the concerns here, and what I wanted to clarify, is the burden of proof is very key for determining how to approach what to do here.

843 Under an industry-specific regime of common carriage, which the policy direction does not undermine in any way, the carrier has the fundamental obligation to engage itself with certain practices that are not unjustly discriminatory and do not give undue preference and section 36 is just a further articulation of the kinds of obligations that a common carrier has.

844 So the fact that they might want to use some practices now that start offering some kind of discrimination it becomes a fact-based inquiry. In what circumstances is treating different customers is that justified or not.

845 In this case common carriage has historically permitted all sorts of flexibility that develops case-by-case as technology evolves to determine under what circumstances is discriminatory treatment unjust or not unjust.

846 The problem here is there seems to be some reticence by the carriers to adequately disclose the full nature of the kinds of traffic management practices they are engaging in and all the uses for which it's done and therefore there is the potential for abuse in how these practices are being utilized to go down the road as to the point where they are unjustly discriminating.

847 So from the consumer group's point of view, there are some practices that may be fully justified, but we don't have enough information to know yet. And these are companies that are not just like any other businesses. Common carriers are not just like any other business and they do have certain constraints from the outset on what practices are permitted that are different from non-common carrier businesses.

848 Thank you.

849 THE CHAIRPERSON: Is just Mr. Lawford's assumption that there will be abuses just because you use DPI I do not share. I mean I posited a very specific question to him, he answered me, he is worried about abuse, which in fairness is your contention. I'm not prepared to assume abuse as you are.

850 But let's go on.

851 Madame Lamarre...?

852 CONSEILLÈRE LAMARRE: Merci, Monsieur le Président.

853 Well, thank you for being here this morning.

854 I have read thoroughly your submission and I must say I did find it very comprehensive so don't be surprised or shocked if my questions are very targeted at getting specific clarification on some of those points. It's not because I'm ignoring the rest of the submission, it's just that that's where I need clarification.

855 So to start off, if we go to paragraph 34 and the following paragraphs also in your initial submission, you state that:

"The consumer groups are concerned primarily that permission to ISPs to make application source destination under categories the basis of their network management, i.e. discrimination, will lead..." (As read)

856 And the first point you bring up is:

"...price discrimination based on these categories..." (As read)

857 MR. LAWFORD: Yes.

858 COMMISSIONER LAMARRE: That's fine. I mean I understand that correctly.

"...with an attendant rise in Internet access pricing for the majority of residential subscribers." (As read)

859 What evidence is available to back up such a statement?

860 MR. LAWFORD: The pricing plans that carriers have at the moment, it's true they are at the level now where it's tiered access and you have, say, three pricing points and that's it. Where that comes from is largely from the DPI vendors own statements of what they can do.

861 The fact that they are selling at telecom conferences to these guys, there are -- and I will be happy to undertake to provide it to the Commission -- but product sheets from Sandvine, Redknee and others that clearly say you can institute individually targeted pricing for, you know, down to a one-to-one ratio.

862 So we have to be forward-looking here. We are concerned that once you have for example the ability to say who is a gamer, again, who is interested in Internet radio, who uses peer-to-peer a lot, that there would be the gamer's package, which coincidentally would cost \$20 more per month than is presently the situation. There would be the package for those that are high-definition YouTube users that costs an extra \$30 a month because you put so much more stress on our network. That kind of pricing would be easy to do now because the DPI equipment already provides that information because it's getting down to which application you are using.

863 So that's possible.

864 COMMISSIONER LAMARRE: Okay.

865 And moving to paragraph 35 -- and I must say that one thing, and that's what I'm getting at here that I'm struggling with is your position in regards to a form of management that would rely on economic models or on pay-per-use, or however you want to call it, pay-per-bit whatever.

866 MR. LAWFORD: Yes.

867 COMMISSIONER LAMARRE: And there seems to be a little bit of contradiction or confusion that I have not been able to settle out.

868 It starts with paragraph 35, where you basically state that:

"Traffic management that is either being discriminatory towards a person or towards a type of content should not be approved by the Commission." (As read)

869 Well, basically just the fact that you have to pay for service is in itself discriminatory. So you are not suggesting that pricing be uniform throughout the country for everybody, either that or adapted to users' income, are you?

870 MR. LAWFORD: No. No.

871 What we are saying is that if you have clearly different usage profiles, usage-based billing, based on the number of bits you drive through the system could be different so I'm going to get a different pricing plan. It's up to carriers if they want to cut me off after 200 GB and say every gigabyte after that is an extra \$3.00. That's possible. That's starting to come.

872 And unless -- what we are saying is, again, that if you are a gamer using gaming programs -- and they know that because of DPI -- that extra charge just because of that is not appropriate because there is no real difference between say, for example, that user and the next-door user who is using a lot of YouTube downloads, they are using the same amount of bandwidth, but you have made a gaming plan which costs more.

873 So they are similarly situated, but they are getting charged differently.

874 COMMISSIONER LAMARRE: Okay. So if an economic model was based on the bandwidth that you use instead of the application that you use within that bandwidth, you wouldn't have an issue with that?

875 MR. LAWFORD: No.

876 COMMISSIONER LAMARRE: Okay.

--- Pause

877 COMMISSIONER LAMARRE: In paragraph 85 you provide some explanation about congestion and then at the end you say -- the last sentence of paragraph 85 you state that:

"However, it is reasonable to assume that peer-to-peer traffic is not anywhere near ..."

878 And I sort of underlined that:

"... anywhere near the magnitude of each http traffic." (As read)

879 Again the same question I asked earlier: What evidence do you have to back up that statement?

880 MR. LAWFORD: That comes from the TELUS numbers that were in the interrogatories

881 COMMISSIONER LAMARRE: Only the TELUS numbers?

882 MR. LAWFORD: The other companies didn't give it to us.

883 COMMISSIONER LAMARRE: Okay.

884 MR. LAWFORD: But the TELUS number is the 3 percent of traffic as opposed to 75 I think it was for http traffic.

885 COMMISSIONER LAMARRE: Okay.

--- Pause

886 COMMISSIONER LAMARRE: Okay. Moving along to paragraph 111.

887 Again this is aimed at my -- this is because of my struggle with your position with regards to an economic model.

888 You seem to be suggesting that if there were such an economic model peer-to-peer users or heavy downloaders or whatever applications that use a lot of bandwidth would be exceeding their monthly limit and overcharged and that's something that you seem to want to avoid. Yet at the same time this morning we heard a statement, at least from Juniper, that 5 percent of users are at any point in time using between 30 to 50 percent of the capacity of the network.

889 So how about trying to create some equity between the users? Why should a user that actually does not make as much use of the network end up subsidizing in a sort of way, shape or form the users that are heavy users?

890 MR. LAWFORD: That kind of equity is desirable because heavier users do put more stress on and should pay more in some models.

891 The question is: Are we going to see, for example, packages from the ISPs lowering prices for Internet service for very light users? I don't think so.

892 What we are saying is that at the present time they have adequate resources and adequate revenue from the charges that they are presently charging people in order to add extra capacity and to handle those heavier users.

893 Now, in the case where amongst other traffic measures they need to put usage-based billing in as a manner of discouraging use or shifting some of it, that's appropriate, but what we are trying to avoid is a situation where bit caps are put on and the prices are -- and those are set quite low and then charges above that are quite high, because this is an unregulated industry so we are concerned that prices will go high quickly.

894 COMMISSIONER LAMARRE: Also, to be fair, like an introduction that led to that conclusion in paragraphs 108 and 109, you did stress out that it's difficult for users to know what kind of bit consumption they are actually doing as opposed to their water or electricity meter, you can go check it out and you know where you are at.

895 MR. LAWFORD: Yes.

896 COMMISSIONER LAMARRE: So if that information was available for each user in a reasonable fashion, would --

897 MR. LAWFORD: That would assist. That would assist greatly because --

898 COMMISSIONER LAMARRE: That would assist, okay.

899 MR. LAWFORD: -- because users could shift their usage and make decisions for pricing plans based on their usage, yes.

900 COMMISSIONER LAMARRE: Okay.

901 MR. LAWFORD: That kind of clarity would be wonderful.

902 COMMISSIONER LAMARRE: Okay.

903 Going back again to peer-to-peer, because that seems to keep a lot of people talking, I just want to make sure I understand your position that peer-to-peer actually does not overload the system in an unexpected fashion, all they do is they use 100 percent of the bandwidth that they are allocated.

904 MR. LAWFORD: It can do so, and in doing so may or may not cause problems for the network depending on the structure of that network, how it's provisioned, whether it's over subscribed or not.

905 But again, it's not for consumers to say my use -- to justify their use. Peer-to-peer users of today may be small, but those of the next generation it there will be everybody and it will be for far more uses.

906 So what we are trying to say with this is that peer-to-peer has to be demonstrated clearly as a problem in that particular network and there has to be justification for proving that that is a different kind of traffic that's something quite out of the ordinary, quite different from, for example, YouTube downloading all day long.

907 COMMISSIONER LAMARRE: Okay.

908 And also in -- okay. I will come back to that later on.

909 In paragraph 132 you do mention that:

"The consumer group considers that operating network capacity is the most user-friendly innovation, creating privacy respecting fashion to deal with traffic congestion." (As read)

910 I don't think anybody is going to dispute that, but it comes with a price tag. And Internet networks, just ask any network, be it an electrical network, public transport networks, water system, even sewage networks, they are designed in an optimized way.

911 So if we were to conclude that a pay-per-use system or an economic system that does not discriminate on the applications or the source of destination was warranted in order to manage Internet traffic, which one of those criteria that you have identified, user-friendly, innovative creativity of privacy respecting criteria, would any of these criteria in your opinion be in jeopardy if an economical model were to be adopted?

912 MR. LAWFORD: No. I don't think any of them in particular would be threatened by that. It would just raise other questions about affordability and the way the pricing plans were presented such that they gave consumers a real choice.

913 But no, I don't think it would have any particular effect on those.

914 COMMISSIONER LAMARRE: Okay.

915 You did mention that one important aspect of traffic management technique was to ensure that consumers, customers, citizens, they knew what they were paying for, what they had bargained for and that in order to do that ISPs should provide detailed description and also notify customers where -- when they changed techniques and give them enough notice so that they would have time to choose to change providers if they wanted to.

916 But a lot of those service providing contracts are usually provided for a specific period of time.

917 MR. LAWFORD: Yes.

918 COMMISSIONER LAMARRE: So do you think that a modification or just any modification in a traffic management technique by a supplier would be reason enough for a consumer to be able to terminate a contract prior to the end of the term of that contract?

919 MR. LAWFORD: We would favour it if there were any ability in any contract to get out of it when there is a major change in terms, because we view that as a fundamental -- I would view that as a fundamental change. If for example all of a sudden YouTube had a different availability, I would view that as changing the contract fundamentally.

920 Whether that is necessary or not, it would be desirable. Even without it I think consumers, if they were informed, would have a long enough memory to think about it when the contract renewal came up. But yes, it's always a problem with these long-term contracts and it would be ideal to have a statement from the Commission saying that a change like that is a fundamental change to the contract and you are now out of it.

921 COMMISSIONER LAMARRE: Well, obviously it would have to be a major change to the technique that's used.

922 So what do you feel -- or have you given any thought to the type of criteria that can lead us to conclude that the change that is done to the technique is a major change?

923 MR. LAWFORD: I haven't put any thought to it before now and hesitate a bit to off the top of my head give you some, but if you will bear with me one moment.

--- Pause

924 MR. LAWFORD: I have just had the thought that if the provider wants to make such a change that they have to give advance notice.

925 But in terms of thinking of other criteria, I would like to beg your indulgence and provide that in an undertaking.

926 COMMISSIONER LAMARRE: Getting now to the test that you have proposed, that is basically very inspired by the Supreme Court test and the Oakes case, you have concluded -- and you were very upfront with it and I appreciate reading documents that are very upfront -- but with their conclusions in paragraph 249 that this test is deliberately high, the test that you have provided that is inspired from Oakes.

927 MR. LAWFORD: Yes.

928 COMMISSIONER LAMARRE: Well, keeping in mind that the Oakes test was developed in order to protect a fundamental right, are you actually saying that what is being looked at in section 36 of the Telecom Act is the equivalent of a fundamental right?

929 MR. LAWFORD: In essence, for customers of a common carrier, yes, because you are saying you expect that traffic to be passed unmolested and it's one of the obligations that they take on in being a common carrier is to pass that traffic.

930 So if we are going to make an application process that lets you around that, that you have to have a similarly

high test, because you are forgoing quite a large consumer right there, the right to have your traffic pass without it being observed or changed, and that is what we are -- that's why we did an equivalent of the two tests.

931 COMMISSIONER LAMARRE: Thank you.

932 Mr. Président, je n'ai plus d'autre question, merci.

933 THE CHAIRPERSON: Len...?

934 COMMISSIONER KATZ: Thank you, Mr. Chairman.

935 Good morning.

936 MR. LAWFORD: Good morning.

937 COMMISSIONER KATZ: Let me start by stating my hypothesis and that is network operators are in business to make money. Network operators operate on a cost and revenue model.

938 Your intervention proposes that carriers not be allowed to control their costs through what I will call network integrity solutions because you are saying they shouldn't be allowed to manage their network by looking at traffic flows and perhaps differentiating between applications and so as a result of that, in the absence of that, their costs will go up. If their costs go up they will have to find a source of revenue for that and that ultimately is the consumer.

939 I guess my question is: Do you have data to support the premise that users are prepared to pay more in order to support a network that is not managed to the extent that perhaps some of the carriers are looking to manage it, notwithstanding the issues of privacy and the issues of spam and denial of service and everything else as well?

940 MR. LAWFORD: I will say that on the public record of this proceeding in a number of the comments which were sent into that comment board there were statements -- and I can find them for you again in an undertaking -- to the effect that I would pay \$140 a month if I got unimpeded access. That's not scientific, but those are statements of real Canadians saying they would pay more. We don't believe that they need to pay more at the moment.

941 COMMISSIONER KATZ: But all things being equal they would.

942 MR. LAWFORD: But let's say carriers -- after a decision where you set out a number of guidelines under section 36 -- prepared their applications, came and said "You know, our network really is in bad shape right now and we do need to put in these application-specific network management practices, at least for the next two years until we change to fibre, everything ethernet, throw out those old DSL switches." You could say "Sure."

943 How does that affect the situation? They will have gone through the process of satisfying you that this exception is necessary to the otherwise quite hard requirement not to fish in packets and not to fish in the message. They just have to prepare an application and come to --

944 COMMISSIONER KATZ: I just want to understand though, you are representing the users in Canada and what I want to make sure is if you are representing them that you are prepared to speak on their behalf and recognize that all things being equal if a carriers' costs go up and they want to maintain whatever profitability or loss they are currently assuming, that the revenues are going to have to go up as well, and, as a result of that, the price to consumers is going to go up.

945 What we have been hearing all along, in the press and everywhere else, is that Canada falls behind the rest of the world on internet usage and on pricing. And if prices are going to go up, that means that demand is going to go down, which goes contrary to where, I believe, this country and Canadians want to go.

946 DR. CHERRY: Commissioner Katz, perhaps I can assist somewhat in answering the question.

947 I think, from your opening statement of assumption, that there may be a misinterpretation of the position that the consumer groups are taking.

948 The consumer groups, as I understand it, and as I am appearing here as an expert on their behalf, are not saying that these carriers cannot engage in network management practices. The problem here is what management practices are appropriate or not. This is where the limitations of common carriage do, in fact, put some constraints on what a carrier can do.

949 However, it is not a blanket rule against them.

950 For example, no unjust discrimination doesn't mean that you can't discriminate at all.

951 Historically, common carriage has been applied, for example, to allow different treatment of different classes of service for different classes of customers, but there has to be justification for why those discriminations are permitted.

952 For example, if there generally is a different cost to the carrier of serving different customers or different types of services, then differentiating among them and how you treat them can be wholly justified.

953 What the consumer groups are saying here is, the problem is that in order to determine to what degree discriminations that may emanate, for example, from network management practices -- to determine which discriminations are just or unjust, we necessarily need more fact inquiry. We need to understand more exactly what these practices are doing and what effect they are having.

954 That is where, under the common carriage regime, and particularly the statutory version -- this is where the burden of proof is really crucial. The burden of proof is on the carrier to justify that it's not discriminatory, but that doesn't mean that they can't make discriminations.

955 All the consumer groups are saying is that, unfortunately, we don't have enough information.

956 Also what is problematic here is, it turns out, if certain attempts were made, such as some of the consumption-based models, as Commissioner Lamarre was talking about -- if you, in fact, made disclosures in advance to customers, for example, that certain kinds of uses, during certain times of the day, or a certain amount is more burdensome, then you actually give the customers the choice to alter their own behaviour, and, in so doing, you may actually obviate, if not eliminate, or at least mitigate the degree to which network management practices have to be even more intrusive to meet their needs.

957 Now, the historical basis for this -- think of voice -- wireline telephony. We traditionally had different pricing plans for heavy users versus light users of long distance. We had peak hours. You paid more during the day than you did for nights or weekends. This was a way to enable --

958 COMMISSIONER KATZ: No, I understand all of that. That isn't what --

959 DR. CHERRY: -- customers to manage, and all we are saying is, unfortunately, what is happening here is that the unilateral nature by which these carriers have invoked these practices has not enabled enough experience to know, in fact, which practices are justified and which are not, in terms of what is really necessary to meet the congestion needs.

960 And this is where I can say, because I have worked for AT&T and Ameritech in the past, a combined 15 years' industry experience -- unfortunately I know, from having worked for these carriers, that they will, for business reasons --

961 THE CHAIRPERSON: Excuse me, but you are really dominating time, and you are not answering the question.

962 DR. CHERRY: I apologize. I was just saying that I do know that there are instances in which they will attempt to use the flexibility they have to generate more revenue, even if it is not necessarily in the best interests of --

963 COMMISSIONER KATZ: Okay. Thank you very much, those are my questions.

964 THE CHAIRPERSON: Tim...

965 COMMISSIONER DENTON: I like where you are coming from, in terms of the common carrier nature of the obligations. I have no problem with that.

966 What I am concerned about is the notion that we, the CRTC, might investigate whether the carrier has made necessary and reasonable investments in regard to making sure that congestion doesn't happen.

967 My concern is (a) I don't know that you are taking congestion seriously enough; and (b) you are asking us to look into other, much less direct ways of handling congestion.

968 There is more than one way to kill a cat than by drowning it in cream.

969 The question I have here -- and you don't have to answer it now, but I would like to see some answer in your argument, is: I don't want us to be involved in making judgments, second-guessing the judgments of carriers about their investment decisions, and I don't want to downplay the issue of congestion as a serious problem that needs to be dealt with, for the benefit of all of us as consumers.

970 Any comment that you want to make on that, now or later, would be most appreciated.

971 MR. LAWFORD: The fact of the matter is, it's not just DPI that you need to use to control congestion. We have suggested other ways, and they don't all involve huge capital investments.

972 We already have a number of internet-based protocols that are probably going to be more detailed in other presentations, but traffic smoothing, early congestion notification, random early drops -- the companies are saying that's not adequate, at least the vendors this morning are saying that's not adequate, because that's not in their interests, because they are selling more.

973 We have content caching, caps on certain users, kicking certain users off if they are extremely high. Those are other things that can be done that don't involve capital investments.

974 It's instructive that TELUS, which is just like Bell, has not seen fit to use DPI, and they are getting along just fine.

975 So there is not necessarily a requirement for capital investment.

976 The other point I would say to that is, they do have, as common carriers, a requirement under the section 7 policy objectives to provide affordable and reliable service, and to meet the needs of Canadians.

977 That has some effect on your thinking, I would hope, as to whether you could specify, at least, some effort being made on their part to upgrade networks, some shred of evidence that there was a plan ahead to not rely on throttling for the rest of time, that they had a strategy, for example, to cut it back hours or cut it back in services they are doing it to.

978 COMMISSIONER DENTON: Point taken; point made.

979 THE CHAIRPERSON: Okay, thank you very much.

980 If you have any further comments, as you know, there is a period until July 24th to make additional comments.

981 Thank you very much.

982 MR. LAWFORD: Thank you.

983 THE CHAIRPERSON: Madam Secretary, over to you.

984 THE SECRETARY: This adjourns the day for today. We will reconvene tomorrow morning at 9:00 a.m.

--- Whereupon the hearing adjourned at 1231, to resume on Tuesday, July 7, 2009 at 0900

REPORTERS

Johanne Morin Jean Desaulniers

Sue Villeneuve Beverley Dillabough

Monique Mahoney Madeleine Matte

Date Modified: 2009-07-06