Initial Comments Of

Campaign for Democratic Media

Telecom Public Notice CRTC 2008-19:

Review of the Internet Traffic Management Practices of Internet Service Providers

23 February, 2009

David Fewer, Acting Director, CIPPIC
Tamir Israel, Articled Student, CIPPIC
Philippa Lawson, Barrister & Solicitor

CIPPIC
The Samuelson-Glushko Canadian Internet Policy and Public Interest Research Clinic
University of Ottawa, Faculty of Law
57 Louis Pasteur Street
Ottawa, Ontario K1N 6N5
613-562-5800 x.2553
cippic@uottawa.ca
www.cippic.ca

Table of Contents

Executive Summary

[1] The internet as we have known it has been an open internet, fundamentally characterized by an architecture that facilitates innovation, encourages freedom, and respects privacy. That architecture is changing.

[2] The traffic management practices scrutinized in this public hearing challenge these fundamental characteristics. These practices are changing the open architecture of the internet into one of control and interference.

[3] Traffic management is justifiable in the presence of network congestion, once that congestion is established by transparent metrics of widely accepted tests.

[4] Traffic Interference – invasive practices that interfere with end user traffic, such as application-based throttling – is not necessary for ISPs to manage network congestion. Traffic Interference should be permissible only transparently, as a last resort, where finely tailored to target congestion, and where implemented in a manner that minimally impairs the user experience, and justified by Queuing Delays predicated on acceptable oversubscription ratios.

[5] It is neither necessary for ISPs to manage network congestion nor appropriate, given the many ways in which it is inconsistent with the *Telecommunications Act* and the fact that feasible alternatives exist.

[6] Preferable options to Traffic Interference should be exhausted before ISPs may justifiably turn to Traffic Interference. These options include:

a. upgrading network capacity – this is the primary response that should be taken by ISPs; the emergence of Traffic Interference among Canadian ISPs is evidence of failure to invest in facilities;

b. demand-based pricing incentives – marketplace structures that return traffic costs to users; and

c. Internet Engineering Task Force-approved traffic management methods.

[7] Internet Engineering Task Force-approved traffic management methods that should assist ISPs in addressing congestion issues include Differentiated Service Labels, Early Congestion Notification, Random Early Drops, Flow-based routing, and "Traffic smoothing" (or "packet grooming"). New traffic protocol initiatives such as "fairness" routing and the P4P Project also show promise as congestion management techniques.

[8] Common Traffic Interference practices include Deep Packet Inspection and RST Injections. These and other Traffic Interference practices should be permissible:

a. only transparently,

b. as a last resort,

c. where finely tailored to target congestion, and

d. where implemented in a manner that:

- minimally impairs the user experience,
- and is justified by Queuing Delays predicated on acceptable oversubscription ratios.

[9] CDM submits that transparency of ISP practices is also fundamental to the legality of traffic management practices. ISPs must be transparent as to:

a. the technical grounds supporting assertions of congestion, including timely and public disclosure of oversubscription ratios and latency rates; and

b. communication of traffic management practices in a timely and clear fashion to both wholesale and retail customers, current and prospective.

[10] Traffic Interference violates the *Telecommunications Act*'s prohibition against "unjust discrimination" because there are other, less invasive/discriminatory ways of dealing with congestion problems.

[11] Traffic Interference violates the *Telecommunications Act*'s prohibition against controlling content or influencing the meaning and purpose of telecommunications by delaying it to such an extent as to render it unusable by users. Because content carried on throttled application communications is qualitatively distinct from other content, application-based throttling burdens such communications in violation of the Act.

[12] Traffic throttling is inconsistent with many of the objectives of the *Telecommunications Act*, including the protection of privacy, facilitating innovation, establishing a reliable system, and meeting user requirements.

[13] Other jurisdictions are grappling with this problem now as well. There is a growing consensus that traffic shaping is undesirable and should be only used as a last resort.

[14] This review of initiatives and approaches in other jurisdictions provides guidance for how to approach this issue in Canada:

a. *Take a holistic approach* – Traffic management is best viewed as part of a long range view of the internet's place in Canada.

b. *Establish clear regulatory rules, not policy statements* – Clear, enforceable rules grounded in the Telecommunications Act, will provide Canadian ISPs, consumers, application developers and content creators and distributors with a secure framework on which to create, innovate and invest.

c. *Treat Traffic Interference as a last resort* – Create incentives for ISPs to invest in capacity rather than Traffic Interference.

d. *Recognize that protocol-agnostic traffic management is possible* – Not all traffic management need amount to Traffic Interference. Canadian ISPs should be encouraged to adopt IETF-endorsed solutions.

e. *Do not permit privacy-invasive traffic management techniques such as DPI* – There are better solutions.

f. *Recognize that throttling undermines competition and choice*.

g. *Require public disclosure of ISP congestion and traffic management practices* – compulsory disclosure of baseline data levels the playing field, enhances consumer choice, permits ISPs to compete on service quality and creates incentives to invest in capacity.

h. Do not demonize P2P technology – It is detrimental to Canadian distributors and creators to cripple this innovative form of distribution.

Introduction

[1] In accordance with the procedure set out in the above-captioned Public Notice, we offer the submissions of the Campaign for Democratic Media (CDM). The CDM is a network of public interest organizations and people that support the development of a truly democratic media system. The CDM is a member of the SaveOurNet.ca Coalition, a coalition of citizens, businesses, and public interest groups fighting to keep the internet a level playing field. CDM is making this submission in support of the SaveOurNet.ca Coalition, and on behalf of citizens from across Canada.

[2] The CDM confirms that it wishes to make an oral submission at the public hearing in this proceeding.

[3] This Comment comprises these written submissions and the following attachments:

a. the testimony of Professor Andrew Odlyzko;[1]

b. the testimony of Professor David Reed;[2] and

c. the testimony of Bill St. Arnaud.[3]

Overview

[4] The internet is of fundamental importance to the Canadian economy, to Canada's cultural and social life, and to Canadians' democratic values.

[5] It might be said that to date, the Canadian portion of the internet has gone unregulated. That view would be mistaken on two levels.

[6] First, a great deal of positive law governs behaviour on the internet, including the behaviour of the commercial actors who build the networks of the Canadian internet. Defamation law, copyright law and Canada's obscenity laws, to name a few examples all constrain the actions of Canadian Internet Service Providers ("ISPs"). These laws can mandate ISPs to engage in particular behaviour – *neutral* behaviour. For example, ISPs' immunity from liability for unauthorized communications to the public of copyright protected works only holds so long as the ISP's activities are neutral as to the content they

---

[1] Testimony of Professor Andrew Odlyzko, Attachment A [Odlyzko].
[2] Testimony of Professor David Reed , Attachment B [Reed].
[3] Testimony of Bill St. Arnaud, Attachment C [St. Arnaud].

carry.[4] Where an ISP has actual knowledge of the infringing nature of the content it carries, or monitoring such content becomes economically and technically practical, the ISP may lose its character as a "conduit" and bear liability.[5]

[7] Second, such a view restricts the meaning of "regulation" to positive law; yet, other forces act as regulators of human behaviour on the Canadian internet. Technology – the architecture of the internet itself – is the single greatest regulator of human behaviour on the internet.

[8] To date, the architecture of the Canadian internet has been open. The individual linked networks that comprise the internet have followed a number of important design principles, including:

a. *Open architecture networking* – The objective of the network design is total connectivity: all vendors, all platforms and all operating systems are treated as equal.[6]

b. *Layered communications* – Communications over the internet occur in mutually independent layers. Applications and content – the user's contribution – occur at a layer independent of underlying layers, such as the physical (the hardware comprising the network) and transport (the Transport Control Protocol) layers.[7]

c. *The End-to-End Principle* – Communications protocol operations occur at the end-points of the network. Protocol operations, such as TCP, are only justified in the lower layers of a network if they optimize network performance.[8]

[9] David Isenberg calls networks based on such principles "stupid" networks, in contrast to the "Intelligent Network" of telephony:

> *The Intelligent Network is a straight-line extension of ...four assumptions ... -- scarcity, voice, circuit switching, and control. Its primary design impetus was not customer service. Rather, the*

---

[4] *Society of Composers, Authors and Music Publishers of Canada* v. *Canadian Assn. of Internet Providers*, 2004 SCC 45, [2004] 2 S.C.R. 427 at para. 92 ["So long as an Internet intermediary does not itself engage in acts that relate to the content of the communication, *i.e.*, whose participation is *content neutral*, but confines itself to providing "a conduit" for information communicated by others, then it will fall within s. 2.4(1)(b)." [Emphasis added] [*SOCAN* v. *CAIP*].

[5] *Ibid*. at para. 101.

[6] See, generally, Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet", *Internet Society* (4 August, 2000) <http://www.isoc.org/internet/history/brief.shtml> [*A Brief History of the Internet*].

[7] *Ibid*.

[8] J. Saltzer, D. Reed, and D.D. Clark, "End-to-End Arguments in System Design", *Second International Conference on Distributed Computing Systems* (April 1981), pp. 509-512; *ACM Transactions on Computer Systems*, Vol. 2, No. 4 (November 1984) pp. 277-288 <http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf>.

> *Intelligent Network was a telephone company attempt to engineer vendor independence, more automatic operation, and some "intelligent" new services into existing network architecture. However, even as it rolls out and matures, the Intelligent Network is being superseded by a Stupid Network,*
>
> - *with nothing but dumb transport in the middle, and intelligent user-controlled endpoints,*
> - *whose design is guided by plenty, not scarcity,*
> - *where transport is guided by the needs of the data, not the design assumptions of the network.*[9]

[10] These architectural characteristics describe a particular kind of network that facilitates certain kinds of behaviour and values. The "regulatory" impact of these architectural characteristics may be summarized as:

a. facilitating unencumbered interaction and communications among individuals and businesses;

b. fundamental to the operation of open and free markets, both for the provision of communications services and in the wider marketplace;

c. enormously stimulative of research, development and innovation in communications services, applications, and beyond;

d. responsive to the economic and social requirements of users; and

e. respectful of the privacy of the individuals.

[11] These behaviours and values resonate strongly with the objectives of the *Telecommunications Act*:[10]

> (a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions;
>
> (f) to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective;

---

[9] David Isenberg, "The Rise of the Stupid Network", *Journal of the Hyperlinked Organization* < http://www.hyperorg.com/misc/stupidnet.html> (originally published in *Computer Telephony* (August 1997), pp. 16-26).

[10] S.C. 1993, c. 38, T-3.4 (as amended), s. 7 [*Telecommunications Act*].

> (g) to stimulate research and development in Canada in the field of telecommunications and to encourage innovation in the provision of telecommunications services;
>
> (h) to respond to the economic and social requirements of users of telecommunications services; [...and]
>
> (j) to contribute to the protection of the privacy of persons.

[12] The traffic management practices scrutinized in this Public Hearing challenge the internet's fundamental architectural characteristics. David Isenberg's "Stupid Network" is being replaced by an "Intelligent Network" that does not heed the design principles of the internet:

a. *No longer open* – Some internet traffic management practices undermine connectivity by burdening particular applications: not all communications are treated equally.

b. *Penetration of communications layers* – Some internet traffic management practices employ Deep Packet Inspection ("DPI)" to violate the application layer in routing traffic.

c. *The End of End-to-End* – Some internet traffic management practices pull routing decisions away from the edges of the network and beyond control of the communication's end-points.

[13] These traffic management practices describe a different kind of network than the open internet that we have come to know and on which the Canadian marketplace relies. Traffic management practices replace the open architecture of the internet with one of control and interference. The "regulatory" impact of a Canadian internet characterized by an architecture of control that, we submit, clashes with the values embodied in the open internet:

a. arbitrary and opaque traffic management practices undermine and impoverish the social and economic fabric of Canada;

b. arbitrary and opaque traffic management practices introduce uncertainty into the marketplace, both in the provision of communications services and in the wider marketplace;

c. arbitrary and opaque traffic management practices introduce risk and so discourage research, development and innovation in communications services, applications, and beyond;

d. traffic management practices are responsive to the economic interests of network providers, no to the economic and social requirements of users; and

e. some management practices invade the privacy of individuals by examining the application layer of communications in which users have legitimate expectations of privacy.

[14] "Traffic Interference" – which we define as invasive traffic management practices such as application-based throttling that interfere with end user traffic – by Canadian ISPs undermines a number of important policy objectives set out in the *Telecommunications Act*. We will return to this theme in our submissions in respect of Question 6 of the Public Notice.

[15] These submissions should not be taken as denying that Canadian internet traffic is changing – it is *always* changing in response to the emergence of the innovations and marketplace developments that the open internet facilitates. The question is how Canadian ISPs should respond to such changes, and when, if ever, should Traffic Interference be accepted as an appropriate response.

[16] We submit that traffic *management* in general is justifiable in the presence of congestion (transparently measured) on the network. However, certain forms of traffic management are inconsistent with telecommunications policy objectives and should not be permitted. *Traffic Interference* is one such form. It is neither necessary for ISPs to manage network congestion nor appropriate, given the many ways in which it is inconsistent with the *Telecommunications Act* and the fact that feasible alternatives exist.

[17] As submitted below in response to Question (2) f), preferable options to Traffic Interference should be exhausted before ISPs may justifiably turn to Traffic Interference. These options include:

a. upgrading network capacity – this is the primary response that should be taken by ISPs; the emergence of Traffic Interference among Canadian ISPs is evidence of failure to invest in facilities;

b. demand-based pricing incentives – marketplace structures that return traffic costs to users; and

c. Internet Engineering Task Force-approved traffic management methods – we see little evidence that Canadian ISPs are exhausting neutral traffic management methods.

[18] Traffic Interference should be permissible:

a. only transparently,

b. as a last resort,

c. where finely tailored to target congestion, and

d. where implemented in a manner that:

- minimally impairs the user experience,
- and is justified by queuing delays predicated on acceptable oversubscription ratios.

[19] CDM submits that Traffic Interference techniques that violate this framework violate the *Telecommunications Act*'s prohibition against "unjust discrimination" and, in some versions, control the content, or influence the meaning or purpose of telecommunications, in violation of section 36(2) of the Act.

[20] CDM submits that transparency of ISP practices is also fundamental to the legality of traffic management practices. ISPs must be transparent as to:

a. the technical grounds supporting assertions of congestion, including timely and public disclosure of oversubscription ratios and latency rates; and

b. communication of traffic management practices in a timely and clear fashion to both wholesale and retail customers, current and prospective.

[21] We are confident that this approach is consistent with the vision of the architects of the open internet, and with the objects of the *Telecommunications Act*. It is also consistent with approaches to traffic management adopted in other jurisdictions.

Question (1) – Internet Growth

a) Growth of Internet Traffic

[22] The Public Notice asks, in Q(1) a):

> *a) How has Internet traffic grown in the past three years and what are the predictions for its growth in the future? What has been the impact on Canadian ISP networks?*

[23] Andrew Odlyzko testifies that worldwide wireline internet traffic growth over the past three years appears to have been in the 50-60% per year range.[11] Professor Odlyzko bases this conclusion on his own studies at MINT and those of the Cisco Visual Networking Index project and of TeleGeography.

[11] Odlyzko, *supra* note 1, at para. 9.

[24] The Cisco study predicts 46% annual growth, internationally, through 2012. Professor Odlyzko suggests that this projected growth rate is credible.[12]

[25] The statistics provided by the carriers in these proceedings that were released to the public show that in Canada, the growth rate has declined from 53% between 2005 and 2006 to 32% between 2007 and 2008.[13]

[26] These studies and disclosures, combined with reported growth rates from other nations (such as Korea, Japan, and Australia) indicate that generally, wireline internet traffic growth rates have been declining.[14]

[27] In Canada, this decline in growth rates cannot be attributed solely to Traffic Interference practices. Telus, who does not engage in Traffic Interference, also exhibits slow growth in average usage. This suggests strongly such users are not ramping up their utilizations very rapidly.[15]

[28] Accordingly, CDM submits that Canadian ISP claims that internet demand growth over the last few years greatly surpassed industry projections are not credible.

[29] On the wireless side, Professor Odlyzko testifies that his review of estimates of global growth are reasonably consistent with the growth reported by Telus in their response to the CRTC interrogatory (130% per year for total traffic, sum of inbound and outbound between May 2007 to December 2008). Other experts project global growth at rates of 100% over the next decade.[16]

b) Average End-User Bandwidth Consumption

[30] The Public Notice asks, in Q(1) b):

> *b) How has average end-user bandwidth consumption changed in the past three years and what are the predictions for future changes in Canada?*

[31] Telus' data indicates that average end-user bandwidth growth for downloads is growing at a faster rate than for uploads.

[32] The Telus data also suggests that the curve is flattening: the top 5% of bandwidth users consuming less than they used to.

---

[12] *Ibid*.
[13] *Ibid.*
[14] *Ibid*., paras. 12-14.
[15] *Ibid.*, para. 13.
[16] *Ibid.*, paras. 19-20.

c) Defining Congestion

[33] The Public Notice asks, in Q(1) c):

> *c) How should congestion be defined in an ISP's network?*

[34] CRTC Public Notice 2008-19, footnote 6, defines "network congestion" as follows:

> *Network congestion is broadly defined to mean a situation whereby the amount of traffic transiting the network may lead to a deterioration of service for some end users.*

[35] David Reed, in his Testimony, suggests that this definition requires refinement. Dr. Reed states that the internet designers have always focused on managing congestion that may arise in the various networks that connect to the internet – what Dr. Reed calls "Autonomous Systems":

> *From the beginning, it has been clear that the ultimate solution of the congestion problem requires that the senders causing the congestion must "slow down" their rate of sending and prioritize their traffic if need be. The network itself cannot eliminate congestion – solving the problem requires cooperation from the senders.*[17]

[36] Dr. Reed moves from this insight to make four points:

a. congestion is intimately linked to Queueing Delay;

b. the user experience of congestion is application dependent;

c. since internet traffic is "bursty", congestion is more properly measured by average Queueing Delay divided by bitrate than by traffic loads between links or Autonomous Systems; and

d. Control of congestion within the internet depends on preventing the buildup of Queueing Delay, and the temporary reduction of continuing inflow into queues that have already formed.

[37] First, Dr. Reed contends that any operational definition of "congestion" in the internet must begin with a definition of "Queueing Delay".[18] Dr. Reed defines "Queueing Delay" as:

> *equal to the total size of the packets waiting in the queue, divided by the data rate of the link that must be used.*[19]

---

[17] Reed, *supra* note 2 at para. 5.
[18] *Ibid*. at para. 6.

[38] Dr. Reed concludes that "congestion" then occurs when the amount of data that must travel through a particular link out of a particular router exceeds the data rate of that link for a long enough period such that a queue builds up.[20]

[39] Dr. Reed notes that Queueing Delay "builds up during bursts of traffic from one or more users, and then gradually goes away" when the users' applications "slow down or go away."

> *When multiple users are communicating over a shared router, not only does the available capacity get shared among multiple users, reducing individual shares, the real problem is that Queueing Delay accumulates, ultimately disrupting the network.*[21]

[40] Bill St. Arnaud picks up on this latter point to establish the fundamental importance of subscription rations to the emergence of congestion on a network:

> *While applications such as P2P file sharing applications might increase the degree to which an individual user may utilize the bandwidth for which she has paid (allowing our 50 customers to use, perhaps, 250 kbps on average instead of the 150 kbps they were using before), this does not mean that the primary cause of the congestion is the user or the application. The primary cause is, rather, the telco/cableco's decision to sell 50 Mbps worth of bandwidth on a port that can only handle 10 Mbps.*[22]

[41] Second, Dr. Reed observes that the congestion is perceived differently by users depending on the application:

> *Most applications tolerate end-to-end queuing delays that are less than 200 milliseconds quite well, and many will tolerate even longer delays. Quality interactive applications such as Voice over IP and interactive videogames have more demanding requirements, and typically work well only when the end-to-end queuing delay is kept below 100 milliseconds.*[23]

[42] Third, Dr. Reed observes that internet traffic is fundamentally "bursty".[24] This causes Queueing Delay even when average traffic demand is below the full capacity of any

---

[19] *Ibid*. at para. 8.
[20] *Ibid*. at para. 9.
[21] *Ibid*. at para. 11.
[22] St. Arnaud, *supra* note 3 , at para. 15.
[23] Reed*, supra* note 2 at para. 14.
[24] *Ibid*. at paras. 15-16.

bottleneck link. Dr. Reed concludes that the variance of the traffic through the link is as important a cause of Queueing Delay as is the total average traffic.[25]

[43] Fourth, Dr. Reed observes that control of congestion within the internet depends on, first, preventing the build-up of Queueing Delay, and second, the temporary reduction of continuing inflow into queues that have already formed.[26] Inflow reduction is accomplished by feedback from congested links causing some or all of the hosts sending data to slow down or to stop sending traffic through that link.[27]

[44] Dr. Reed concludes:

> *So to summarize the points made in answer to this question, congestion in an ISP is best defined (1) in terms of average Queueing Delay (in seconds) caused by the properties of all competing traffic sharing common links, and (2) by how quickly a congested link can signal enough of the hosts whose traffic causes the congestion to reduce their sending rate for a period of time needed to drain the queue of its current data and all of the data already "in flight" from the source host.*[28]

[45] With respect to "all competing traffic sharing common links", we note Bill St. Arnaud's observation that the "primary cause of congestion" is "but the practice of [carriers] selling more bandwidth than they are willing to provision for."[29]

[46] We conclude from this analysis that "congestion" must be defined as unacceptable Queuing Delays predicated on acceptable oversubscription ratios.

d) Applications, Services and Congestion

[47] The Public Notice asks, in Q(1) d):

> *d) Are there applications or services that are more likely to cause congestion, and if so, what are they?*

[48] Andrew Odlyzko rightly points out that the first question to address is which applications are vulnerable to congestion. Professor Odlyzko states that these are "primarily voice telephony and video telephony (including videoconferencing), where real-time human interaction is involved."[30]

---

[25] *Ibid.* at para. 18.
[26] *Ibid.* at para. 19.
[27] *Ibid.* at para. 20.
[28] *Ibid*. at para. 22.
[29] St. Arnaud, *supra* note 3, at para. 49.
[30] Odlyzko, *supra* note 1, at para. 24.

[49] Video – often offered as the justification for Traffic Interference practices – is surprisingly resilient:

> *Almost all video, on the other hand, can be handled successfully on the public Internet, and is surprisingly resistant to congestion. This can be done by using progressive downloads, as is used by YouTube and many other video delivery services, and avoiding real-time streaming.*[31]

[50] Video streaming, thus, is not a real-time application. The vast majority of video applications on the internet are, in fact, progressive downloads which handle congestion well.

[51] In terms of the applications that consume bandwidth, Professor Odlyzko testifies that:

> *video dominates in terms of volume of traffic, and this video is delivered over either peer-to-peer (P2P) software, or by content delivery networks (CDNs) like Akamai, or directly from various servers.*[32]

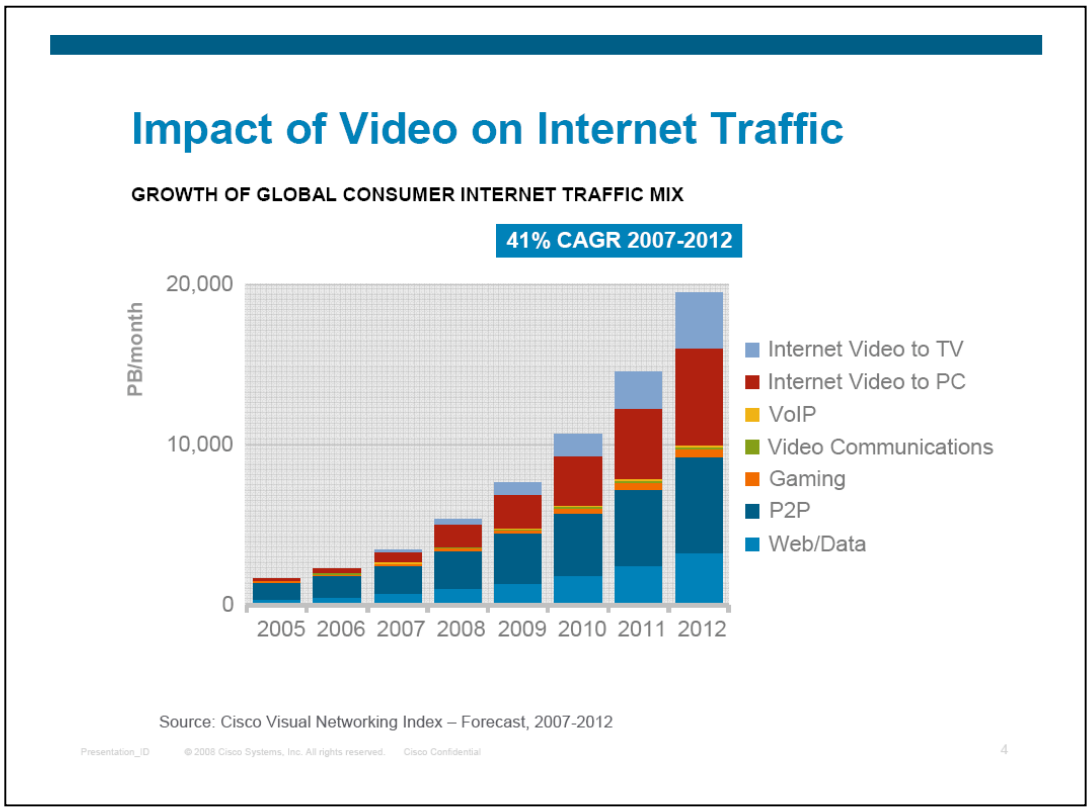
[52] Professor Odlyzko observes that BitTorrent files occupy both upload links and download links, and can utilize bandwidth efficiently. However, note that file size does not change with the application used: a video clip is the same size whether communicated by progressive download or by BitTorrent. As Professor Odlyzko notes:

> *in principle any transmission can cause congestion. A web page with rich graphics can be just as serious a contributor to congestion as a movie (although usually for a much shorter period).*[33]

[53] Professor Odlyzko's take is the same as that reported by third parties. Reproduced below is a chart from Cisco projecting future consumption of global bandwidth.[34] While Cisco predicts growth in P2P traffic, that growth is modest compared to the growth Cisco projects for online video:

---

[31] *Ibid*.
[32] *Ibid*. at para. 25.
[33] *Ibid*.
[34] Cisco Visual Networking Index – Forecast, 2007-2012 (16 June, 2008) <http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf>



e) Application Bandwidth Requirements

[54] The Public Notice asks, in Q(1) e):

> *e) What are the relative bandwidth requirements for different types of Internet applications?*

[55] Andrew Odlyzko observes that bandwidth requirements for video are often overstated:

> *resolutions of movies and video clips are not likely to grow very rapidly, due to limitations on display technologies. On the other hand, transmission speeds should grow. 100 Mbps is already routinely available in Japan and South Korea, and South Korea has recently announced a national goal to make 1 Gbps available almost universally in a few years. In an environment where such high speeds are available, access links will likely be very lightly utilized, and congestion will arise from coincidence of rare events. P2P will be one contributor to congestion, but just one, and may very well not be the main one.*[35]

[35] *Ibid*. at para. 27.

[56] Bandwidth demands of those few applications that demand low latency vary with the application. High-end video-conferencing is potentially high-bandwidth, requiring up to 10Mbps. However, a good user experience can be had for as low as 1Mbps, and basic video telephony can be done successfully at a few hundreds of kilobits per second. However, a good user experience requires on the order of 1 Mbps, and high-end video conferencing systems can take over 10 Mbps.[36]

[57] VOIP bandwidth requirements are surprisingly modest. As Professor Odlyzko states:

> *Voice telephony can be carried in compressed form, with some loss of fidelity, as is done currently in the commercial wireless sectors, at rates on the order of 10 Kbps. However, to assure high quality with minimal latency, many VoIP services encode it as the basic 64 Kbps rate of PSTN or even somewhat higher. However, even addition of stereo and quality higher than the "toll quality" of PSTN is unlikely to require more than 20 Kbps.*[37]

[58] Online gaming comprises surprisingly low overall traffic. Most processing is done locally and data required for generating video images is often locally stored. However, the transmissions that occur come in bursts and require lower latency than for either voice or video.[38]

Question (2) – Technical and Economic Solutions for Traffic Management

a) Traffic Management Technologies

[59] The Public Notice asks, in Q(2) a):

> *a) What technologies could be employed by ISPs (for example, deep packet inspection) to manage Internet traffic?*

[60] Dr. David Reed divides the world of traffic management technologies into two categories:

a. "Traffic management technologies", which are consistent with IETF standards for routing internet traffic, and

b. "Traffic Interference technologies". Traffic Interference technologies:

- selectively or arbitrarily restrict traffic associated with certain sources, destinations, content types, applications or protocols,

---

[36] *Ibid*. at para. 29.
[37] *Ibid*. at para. 28.
[38] *Ibid*. at para. 30.

- are based on information not provided by the customer host or application for use in shaping (in other words, they looking inside the content, rather than at the envelope), and
- do not following the standard mechanisms for signalling congestion.[39]

[61] Dr. Reed identifies a number of IETF-approved techniques for managing traffic. These include:

a. Diffserv ("Differentiated Service Labels") - This is a labelling or marking of packets that allows the endpoints to specify which packets can tolerate delays or reduced priority for capacity. This technique allows users to fine tune their needs – essentially akin to labelling packets as "express", "second class", "ground", etc. – and communicate those needs to ISPs so that they can be "fair" in a way that is informed by the application needs.[40]

b. ECN ("Early Congestion Notification") – ECN is a standard method for marking envelopes that pass through congested regions of the network that permits endpoints to determine whether or not to slow down without discarding traffic.[41]

c. RED ("Random Early Drops") – RED is a standard method for networks to signal congestion by randomly discarding packets before a queue builds up, signalling endpoints to slow down.[42]

d. "Flow-based routing" – This refers to rerouting flows in order to rebalance load when alternative paths are available to the destination. Flow-based routing is generally appropriate for persistent levels of congestion.[43]

e. "Traffic smoothing" (or "packet grooming") – These are broad terms describing a range of equipment based techniques for spacing out packets so that they are less "bursty". Although not specifically IETF they are not viewed by anyone at IETF as problematic when applied to all packets arriving on a physical link so long as they remain blind to source, destination, content, and application.[44]

[62] Other techniques commonly used to "manage" internet traffic are Deep Packet Inspection (DPI) and RST Injection. Dr. Reed identifies DPI and RST Injection as Traffic Interference. DPI and RST Injection violate IETF standards:

---

[39] Reed, *supra* note 2 at para. 30.
[40] *Ibid*.
[41] *Ibid*.
[42] *Ibid*.
[43] *Ibid*.
[44] *Ibid*.

> *Neither Deep Packet Inspection nor RST Injection are standards, and are not acceptable behavior by Autonomous Systems in the Internet, for a simple reason: they each violate the expectation that the contents of the envelopes are untouched inside and between Autonomous Systems, and delivered by best efforts. TCP RST injection is problematic because it is supposed to mean "the other end of the connection has failed" dropping packets/datagrams when there is no actual congestion.*[45]

b) Traffic Protocol Developments

[63] The Public Notice asks, in Q(2) b):

> *b) What developments are under way with respect to traffic protocol (such as modifications to transmission control protocols) and/or application changes (such as changes to P2P file exchange) which could assist in addressing network congestion?*

[64] Dr. Reed argues that congestion control techniques can only work well "if they are standardized across the internet." Generally, such techniques are developed slowly, typically under the auspices of the IETF, and introduced carefully.[46]

[65] Dr. Reed notes that traffic control is the domain of TCP:

> *Responsibility for indicating priority and slowing down traffic is part of the standard end-to-end protocols, in particular TCP. TCP responds to such notification by rapidly slowing down its transmission. All file transfers, including BitTorrent, use TCP, so when congestion is detected, the senders slow down.*[47]

[66] New research in the area is focusing on notions of "fairness" as to how the degree of "slowdown" is allocated among distinct end-to-end flows on the network.[48]

[67] "Fairness" is a difficult concept, as users have diverse needs and applications diverse demands.

[68] Another initiative that deserves mention is the P4P Project. This project seeks to improve peer-to-peer applications' impact on congestion by modifying the peer selection process to prefer nearby peers, thereby minimizing the application's cost to ISPs and reducing overall congestion on the ISP's network.[49] The P4P Project amounts to a co-operative approach to

---

[45] *Ibid*. at para. 36.
[46] *Ibid*. at paras. 44-45.
[47] *Ibid*. at para. 46. See, generally, B. Briscoe, "Flow Rate Fairness: Dismantling a Religion", 37(2) ACM SIGCOMM Computer Communications Review (2007) at 65 < http://ccr.sigcomm.org/online/?q=node/172 >.
[48] Reed, *supra* note 2 at para. 47.
[49] See, generally, Yale P4P Project < http://codex.cs.yale.edu/avi/home-page/p4p-dir/p4p.html >.

responding to the impact of the efficiencies of BitTorrent communications on ISP networks.

c) Capabilities of Technical Solutions

[69] The Public Notice asks, in Q(2) c):

> *c) What are the specific capabilities offered by the technical solutions identified in (a) and (b) above? For example, would these technologies allow for throttling of individual users or groups of users; would they allow for the collection of information about persons and to what extent?*

[70] Queue Drops control the default end-to-end congestion. This functionality signals congestion to the endpoints, resulting in amelioration of the effects of unresponsive traffic sources. [50]

[71] Diffserv – "Differentiated Service Labels" – allows endpoints on the internet to indicate their desired prioritization of data flows, thus facilitating a choice of packets to delay. [51]

[72] ECN signals congestion early in its emergence, facilitating more rapid and stable responses by the sources.[52]

[73] RED also provides early signaling of congestion, thus facilitating more rapid and stable responses by the source.[53]

[74] Flow-based smoothing enables better use of internal resources. This technique also reduces the load on the congested ISP by diverting traffic to alternate available paths through other uncongested networks on the internet.[54]

[75] Traffic smoothing (packet grooming) eliminates unnecessary bursts of traffic that would cause unnecessary short-term congestion.[55]

[76] Traffic Interference techniques also address congestion issues. Deep Packet Inspection advocates claim the technique offers the benefit of inferring traffic priorities by reading content of packets. Other benefits claimed have to do with eliminating unwanted traffic such as "spam", viruses, and "copyright infringing" content. Dr. Reed cautions that the

---

[50] Reed, *supra* note 2 at para. 50.
[51] *Ibid*. at para. 53.
[52] *Ibid*. at para. 55
[53] *Ibid*. at para. 54.
[54] *Ibid*. at para. 56.
[55] *Ibid*.

actual benefit depends on reliability of inference of content type and application requirements.[56]

[77] RST Injection, another Traffic Interference technique, is said to offer the benefit of permitting management of aggressive traffic sources that will not respond to ordinary standard mechanisms. Dr. Reed notes the RST Injection is likely disruptive to many standard applications, and depends on the reliability of Deep Packet Inspection.[57]

[78] Traffic protocol developments also offer specific advantages. "Fairness-based" traffic routing potentially offers a mechanism to more efficiently divide bandwidth among traffic based on "fairness" criteria. This proposal involves an open standard that will be vetted by the entire internet community.[58]

[79] P4P proposes to change the demands imposed on ISPs by popular applications. This offers both consumers and ISPs efficiency and cost benefits. P4P also proposes an open standard that may be adopted by any application publisher and be understood by any ISP. This approach may significantly alleviate congestion attributable to P2P traffic.[59]

d) Effectiveness of Technical Solutions in Addressing Congestion

[80] The Public Notice asks, in Q(2) d):

> d) With reference to questions (a) to (c) above, how effective would these solutions be in addressing network congestion in the ISP networks?

[81] Existing standards and tools, if more widely used, could dramatically reduce congestion. Dr. Reed notes that:

> *All of the standard solutions already provide very effective tools that can dramatically change congestion. In particular, traffic management, diffserv and ECN, which are not widely deployed today, can have significant effects if hosts make use of them as designed.*[60]

[82] It is less clear the extent to which non-standard Traffic Interference techniques address network congestion. Throttling traffic obviously has the effect of reducing traffic on the network – but the important question is the extent to which the practice addresses congestion while simultaneously meeting user needs. A perfectly throttled network is

---

[56] *Ibid*. at paras. 57-58.
[57] *Ibid*.
[58] *Ibid*. at paras 46-48.
[59] *Ibid*. at para. 49.
[60] *Ibid.* at para. 59.

perfectly uncongested – and perfectly useless. Application-based throttling makes assumptions about consumer requirements and priorities that may be false.[61]

e) Technical Solutions, Interoperability and IETF Standards

[83] The Public Notice asks, in Q(2) e):

> *e) Also with reference to questions (a) to (c) above, what impact could the implementation of technical solutions have on the Internet Engineering Tark Force standards upon which the operation of the Internet is based? Could these solutions create interoperability challenges for application developers?*

[84] Queue drops, Diffserv, ECN, RED and flow-based routing are fully compliant with IETF standards. Because these standards are developed openly, as application issues arise they may be addressed by the community. This model leads to improved functioning of the internet as a whole as solutions are adopted by other ISPs within the internet.[62]

[85] Traffic smoothing and packet grooming are compliant with IETF standards and present no interoperability challenges for application developers.

[86] Caching is compliant with IERT standards and presents no obvious interoperability challenges for application developers.

[87] Deep Packet Inspection and RST Injection are not compliant with IETF standards, and are implemented by ISPs in a confidential manner. As Dr. Reed notes:

> *If each ISP implements unpredictable and secret congestion management techniques, application developers will not be able to design applications that work equally well on all parts of the Internet, and diagnosing problems seen by users will become much more difficult or impossible.*[63]

f) Advantages and Disadvantages of Traffic Management Practices

[88] The Public Notice asks, in Q(2) f):

> *f) Describe the advantages and disadvantages (**including end-user impacts**) of employing the following practices in order to manage Internet traffic:*
>
> *i. monthly bandwidth limits (bit caps),*
> *ii. excess bandwidth usage charges*

---

[61] *Ibid.* at para. 61.
[62] *Ibid*. at para. 64.
[63] *Ibid*. at para. 62.

iii. time of day usage pricing
iv. peak period throttling
v. end-user-based throttling
vi. application-based throttling,
vii. content caching
vii. upgrading network capacity, and
viii. others not listed above

[89] Application-specific throttling is undesirable as a traffic management technique. There are alternatives to managing traffic that are equally feasible and far more suitable. This section will list available network management techniques and examine the various advantages and disadvantages of each. This discussion is divided into three sections.

[90] The first addresses the utility of managing network traffic through expansion of network capacity alone. It highlights evidence showing that reasonable investment in internet infrastructure would be sufficient to address current and future projections in traffic growth.

[91] The second focuses on demand management mechanisms such as pricing schemes aimed at encouraging user self-regulation. It argues that, while these should not be resorted to yet, if provisioning becomes insufficient in meeting network needs, pricing incentives should be the next recourse of ISPs. Some pricing schemes are more desirable than others, while some should be avoided altogether.

[92] The final section analyzes various technical measures ISPs can take to manage traffic in order to reduce congestion. It argues that technical traffic shaping mechanisms should only be permitted as a last resort response to growing traffic. It proceeds to analyze the advantages and disadvantages of different available mechanisms.

i) Upgrading network capacity

[93] While the majority of ISPs still claim that provisioning remains their primary response to traffic congestion on their networks, many argue that there is cause to deviate from this norm. In assessing the advantages and disadvantages of provisioning, it is important to first understand why ISPs argue that provisioning is no longer sufficient as a sole response to congestion on their networks.

[94] These arguments include the following: ISPs claim that traffic growth projections indicate exponential increases in internet traffic that will fast outpace any reasonable attempt to keep up through investment in infrastructure alone. ISPs also imply that the nature of certain types of user-generated traffic is such that expanding network capacity will not sufficiently alleviate congestion. Some ISPs further claim that certain types of network traffic take advantage of existing traffic management in a manner that diverts a

disproportionate amount of traffic to the users generating that traffic and are therefore unfair. Each of these claims will be addressed below.

[95] Some ISPs point to projections of exponential growth in internet traffic expected in the near future to demonstrate that it would take exorbitant amounts of investment in network capacity to meet this growing demand.64 Bell, for example, argues that in order to meet growing demand in North America, an additional investment of up to $43 billion will be required by 2010.65 ISPs point specifically to expected dramatic increases in video distribution.66 Based on these projections, ISPs conclude that "the reason behind network congestion is the dramatic increase in demand relative to capacity" and, further, that "[y]ou can never build your way out of this problem."67

[96] The ISPs seem to ignore the fact, pointed out by Dr. Odlyzko out in his testimony attached to this submission, that:

> *[h]istorically, over the last decade and a half, there have been several waves of concern that various disruptive innovations would swamp the Internet and require the introduction of intrusive control mechanisms on customer usage.*[68]

[97] Dr. Odlyzko challenges projections of exponential growth and states that increases in video-driven traffic are unlikely to pose the threat to the Internet that many claim. Commenting on Nemertes projections relied upon by ISPs to justify investment predictions of $43 billion by 2010, Professor Odlyzko states that such claims "have not provided any evidence of their estimates."69

[98] Professor Odlyzko's forecasts are based on current growth rates in Canada and worldwide, which appear to have been slowing down to about 50-60% per year over the past three years. Based on these, Professor Odlyzko refutes ISP claims that recent traffic growth has vastly surpassed industry expectations.70 He concludes that these declining growth rates do not produce a problem of such proportions that 'cannot be built out of'. In fact, when continuing improvements in technological efficiency are factored in, Professor Odlyzko

---

[64] Bell, 2008-108 submissions, July 11.
[65] *Ibid*. at para. 67.
[66] *Ibid.* at para. 53.
[67] *Ibid.* at para. 64 and Comcast SVP Joe Waz, 27 March 2008. See also statement by Rogers' Chief Strategy Officer that "You can't spend your way out of this problem", Peter Nowak, "*Rogers says its internet interference is necessary, but minimal*" 10 June 2008, CBC News, online: http://www.cbc.ca/technology/story/2008/06/10/tech-rogers.html, respectively.
[68] At p. xx
[69] At p. 2.
[70] P. 3

concludes that ISPs can meet projected growths in demand with mild infrastructure investment.71

[99] Some ISPs argue that the nature of certain types of traffic is such that increasing network capacity will not provide a solution to the problem. Most of these arguments target the P2P protocol directly.

[100] Arguments targeting the P2P protocol include the following claim:

[101] Some P2P file-sharing applications constantly look for the fastest node available, and thus any increase in capacity to one network node will attract increased P2P file-sharing upload requests from other P2P file-sharing applications resident on other networks. As described by Rogers' Chief Strategist at the latest Telecom Summit, Rogers' tests have indicated that an increase of capacity at a node could be eaten up by P2P file-sharing applications within 24 hours. Indeed, [Bell's] own testing shows that in some cases the increase in capacity could be eaten up in as little as 30 minutes. Additional capacity cannot, on its own, resolve this issue.72

[102] Other ISPs make similar claims that P2P applications "by their very nature, consume all available bandwidth capacity to complete the upload."73 There is some truth behind such claims, but some clarification is required on this point.

[103] First, it should be noted that stating that P2P applications will 'eat up' increases in capacity within 24 hours or 30 minutes is deceptive. The amount of time it takes for an increase in network capacity to be 'eaten up' is largely a function of how much capacity has been added. A 10 kb upgrade at any congested DSLAM port is likely to be 'eaten up' in even less time than 30 minutes, and this will be the case even if there is zero P2P traffic on that port.

[104] Second, this claim is true insofar as increasing network capacity at a given node will attract more downloaders from around the world. However, it should be noted that there is an upper limit to this phenomenon. ISP customers will never be able to upload more bandwidth than the ISP has sold to them. As Bill St. Arnaud points out, ISPs sell significantly more bandwidth to customers than they are willing to provision for in their networks.74 The fact that increasing network capacity at a given node will lead to an increase in traffic results to a great extent from ISPs' oversubscription practice. Expanding network nodes will cause consumers on that network to utilize a higher proportion of the upload bandwidth they have purchased from the ISP, but there is a upper limit to the total

---

[71] P. 4.
[72] Bell 2008-19 interrog response to Q. 8 at p. 13 of 23.
[73] Shaw 2008-19 interrog response to Q.8.
[74] Testimony of Bill, generally

bandwidth that can be consumed at any given time, equal to the aggregate amount of bandwidth that the ISP has sold to its customers.

[105] Realistically, however, this upper limit will never be reached. As Professor Odlyzko points out in his testimony, consumers generally utilize only a small proportion of the overall bandwidth available to them over a given period of time. So, for example, Professor Odlyzko estimates that the average consumer in Canada will utilize approximately 2% of her full monthly bandwidth allowance.75 It is unlikely that increasing network capacity will attract enough downloaders to push this number to 100%. Indeed, the data from Telus, a Canadian ISP that does not throttle uploads, and so can be expected to provide high upload speeds, shows that outbound traffic at its network backbone has not increased substantially over the past couple of years.76 While Telus does employ pricing incentives to discourage aggressive bandwidth use, these numbers strongly suggest that increases in upload bandwidth capacity at network nodes will not lead to the infinite growth in traffic that some ISPs claim they might.

[106] ISPs argue further on this point that much of the additional P2P traffic that will be attracted from increasing capacity at a node on their networks will come from non-customers. The image, espoused by Rogers in its interrogatory responses , of its network becoming "overwhelmed by the tens of millions of Internet users who are not Rogers customers" is problematic in two respects.77 First, global P2P downloads target the fastest nodes available. Expanding some capacity on Canadian networks is not likely to propel either Canada in general or Rogers specifically to the position of 'fastest network in the world', especially without the addition of FTTH.

[107] More importantly, however, this type of rationale runs counter to the essence of both the P2P protocol itself and the Internet more broadly. Rogers suggests that its customers do not benefit from expanded upload capacity. However they do, insofar as the P2P protocol is based on symmetrical sharing. So for every Mb of download by a Rogers' customer, there must a corresponding Mb of upload somewhere on the internet. As such, Rogers customers who use P2P rely, on a macro level, on the availability of equivalent upload capacity. If all ISPs globally attempted to act as Rogers and other Canadian ISPs are by attempting to minimize P2P uploads from their networks, than P2P will not work effectively for anyone, including Rogers' customers. If this type of 'every ISP for itself' reasoning were to become the norm, it will seriously deteriorate the ability of the Internet to function effectively.

---

[75] P. 6.
[76] Telus Interrog Q1, p. 2 of 6.
[77] Rogers Interrog, Q8, p. 3/4.

[108] Arguments of this nature therefore hold no water as justifications for failing to provision adequately in response to traffic growth. Increasing network capacity does not necessarily entail extensive and unreasonable costs. And P2P traffic growth is not of such a nature that it cannot be addressed through network expansion alone.

[109] The advantage of provisioning as the primary response to traffic growth is that this would furnish Canada with an enhanced Internet infrastructure, a good in itself.78 A Canadian traffic management strategy that focuses on provisioning would be particularly advantageous in light of the fact that Canada appears to be falling behind in Internet capacity.

[110] While no ISPs have publicly disclosed infrastructure investment in this hearing, comparisons may be made internationally on a number of fronts that, taken together, support this conclusion. These comparisons include:

[111] Metrics of broadband subscribers per 100 inhabitants;

[112] Metrics of percentage of subscribers with high speed connections; and

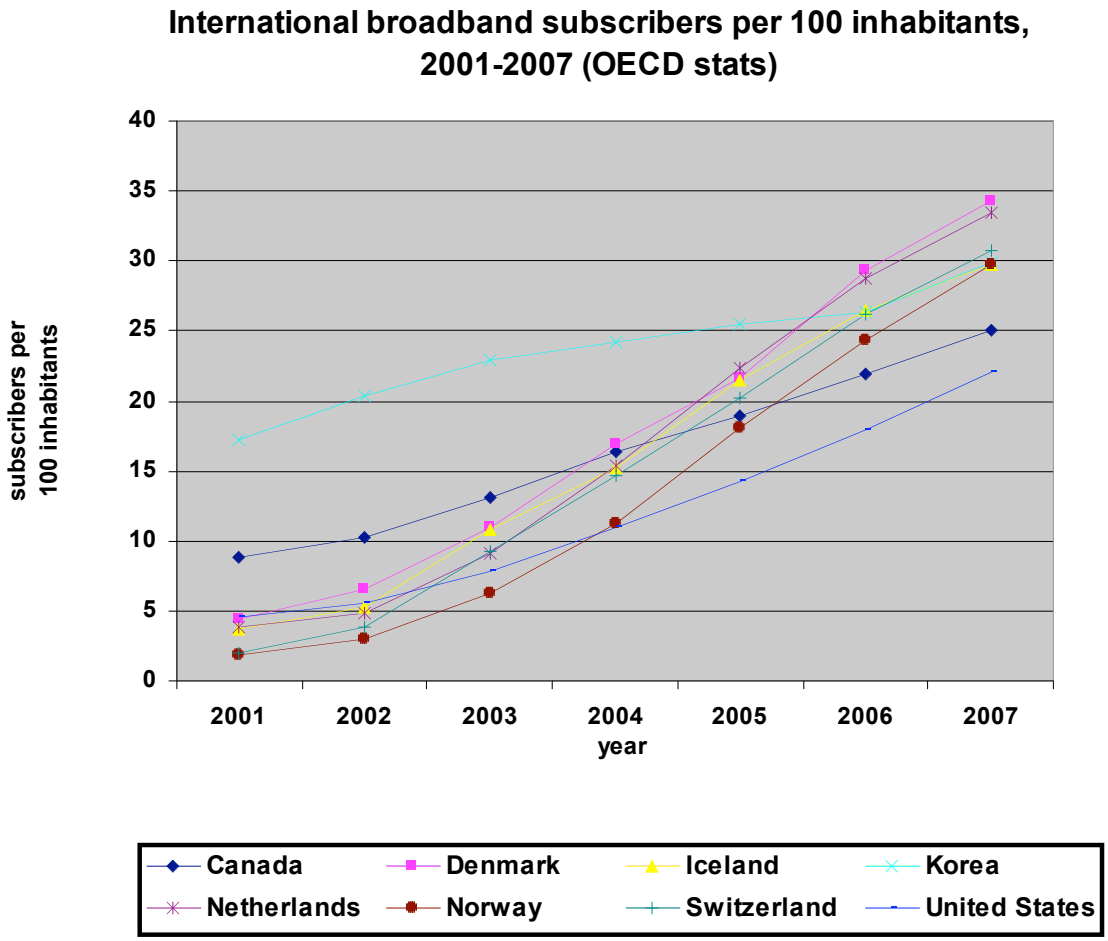
[113] An Oxford study's assessment of broadband quality.

[114] OECD data indicates that Canada has lost its leading position in broadband penetration and is in fact falling behind other nations. OECD statistics indicate that although Canadians were among the early leaders in broadband adoption, second only to South Korea from 2001 through 2003, as of June 2007, adoption rates in South Korea, the Netherlands, Switzerland and Scandinavian countries had overtaken those in Canada. The following chart, derived from OECD data, indicates that Canada fell to ninth overall by 2007.79

---

[78] Get Reference: Internet is good!

[79] OECD Broadband Statistics to June 2007 <http://www.oecd.org/document/60/0,3343,en_2649_34225_39574076_1_1_1_1,00.html>.



[115] Second, Akamai Technologies' observations on national high-speed broadband penetration suggests that Canada lags behind its peers. Akamai facilitates content distribution over the internet for its customers, and is well placed to make these observations – it handles billions of online communications daily.80

[116] Akamai Technologies' State of the Internet Report, for Q3, 2008, reports on "broadband" – connections greater than 2 Mbps – and "high broadband" – connections 5 Mbps or greater. Akamai classifies as "narrowband" connections slower than 256 Kbps. Akamai bases its rankings on actual observed connections to the Akamai network (unique IP's per capita). Canada ranked only fifteenth, not only behind global leaders Japan and South Korea, but also behind the United States and many European countries:81

---

[80] About Akamai < http://www.akamai.com/html/about/index.html> ("We play a critical role in getting content from providers to consumers. … Our global platform of thousands of specially-equipped servers helps the Internet withstand the crush of daily requests for rich, dynamic, and interactive content, transactions, and applications… Today Akamai handles tens of billions of daily Web interactions for companies…").

[81] Akamai Technologies' *State of the Internet Report*, for Q3, 2008 <www.akamai.com/stateoftheinternet>.

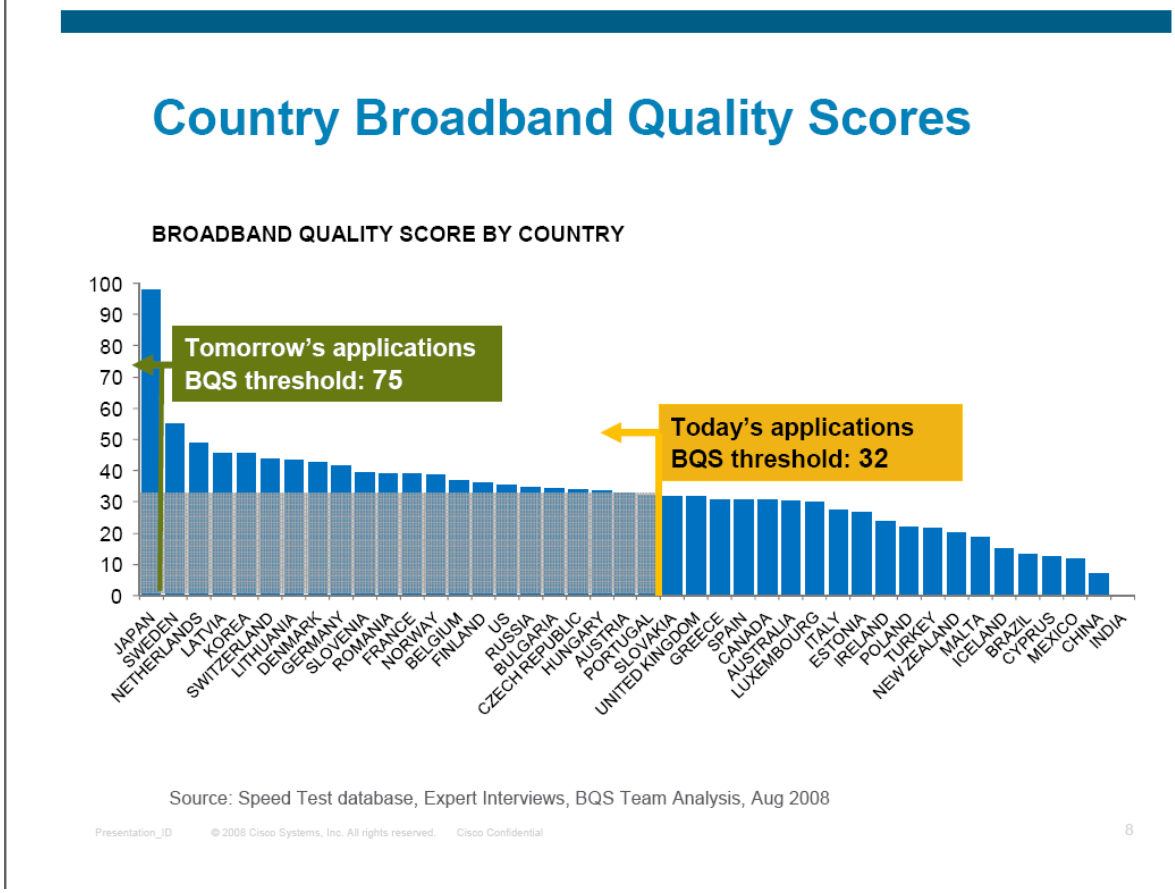
Rank	Country	% above 5 mbps
1	South Korea	58%
2	Japan	55%
3	Romania	43%
4	Hong Kong	38%
5	Sweden	37%
6	Belgium	29%
7	Denmark	27%
8	US	26%
9	Singapore	26%
10	Netherlands	25%
11	Switzerland	21%
12	Canada	21%
	Global	19%

[117] Third, a recent survey conducted by the Oxford Said Business School in London and the Universidad de Oviedo in Spain ranked countries by a broadband quality score (BQS), a measure of the proliferation of high-speed internet in a country, as well as the speeds available and the reliability of connections. Scores were calculated by testing download and upload speeds in each country, as well as latency.82

[118] The study's authors argued that in order to meet the demands of today's internet traffic, broadband networks need to be able to deliver steady download speeds of 3.75 megabits per second and uploads of 1mbps with a latency no greater than 95 milliseconds – a raw BQS of 32 (55% Download + 23% Upload + 22%Latency).

[119] The study's authors ranked Canada 27th out of 42 countries, with a raw score of just under 32 – beneath the threshold:83

[82] Oxford Said Business School and Universidad de Oviedo, Broadband Quality Score (September, 2008) <http://www.sbs.ox.ac.uk/downloads/Broadband_Quality_Study_press_presentation.pdf>.
[83] *Ibid*. at 8.



[120] Even factoring penetration into the mix, the study's authors still concluded Canada was among those nations playing "catch-up" – no longer among the leaders.84 This lack of developed Internet infrastructure may be a main reason why Canadians pay more per Mb of bandwidth than most other comparable countries.85

[121] In addition, investment in infrastructure is a fair response by ISPs to traffic growth. As Bill St. Arnaud testifies, oversubscription is a standard practice of ISPs. This means that ISPs sell more bandwidth then they have provisioned for throughout their networks.86 To some extent, this is reasonable. No consumer will use their entire allotment of bandwidth for any extended period of time. It would be excessive for ISPs to provision their networks to handle every Mbps they sell. However if, due to some technological innovations such as the development of the P2P protocol, some customers of ISPs begin to use a higher proportion of their allotted bandwidth , it is incumbent on ISPs to increase their capacity accordingly. This is only fair, given what the ISP promised to its customer. Provisioningis thus the fairest response to increasing traffic. The consumer who has paid for a certain amount of bandwidthshould be able to use what she has paid for.

---

[84] *Ibid.* at pp. 10-11.

[85] Information Technology & Innovation Foundation, 2008 ITIF Broandband Rankings, available online at: <http://www.itif.org/files/2008BBRankings.pdf>. This study ranked the amount of money Canadians have to pay per Mbps of bandwidth second highest among the 20 leading nations, with only Iceland ahead.

[86] Testimony of Bill St. Arnaud, February 23, 2009, Attachment C, generally.

[122] Finally, increasing network capacity is by far the least intrusive response to increased traffic available. It requires no deviation from the underlying standards that have guided the Internet from its inception.87 While perhaps there are cheaper alternatives, provisioning is also the simplest response, as Dr. Reed points out:

> *One should note that a very simple way to avoid complex congestion management is to make sure that the capacity of individual links is significantly larger than the peak average traffic of all users. Clearly building in too much overcapacity is costly, but attempting to operate links at nearly full capacity will ensure that unacceptable congestion is constant.*[88]

In addition, provisioning best fulfils key objectives of telecommunications in Canada, as embodied in s. 7 of the Telecommunications Act.89

[123] In sum, increasing network capacity is by far the best response to addressing traffic growth. Current growth levels demonstrate that with reasonable investment in infrastructure, ISPs can dramatically reduce congestion, refuting ISP claims that this strategy is not feasible.90 Provisioning as opposed to throttling will also benefit all Canadians and put Canada back on track to be among the top countries in Internet capacity. It is also the fairest response ISPs can provide. Finally, investment is the least intrusive response and furthers many key telecommunications objectives. For all these reasons, provisioning should be the first and primary response to network congestion. Any steps beyond provisioning should occur only in "exceptional circumstances".91

ii) Pricing incentives

[124] CDM submits that the best response to congestion is provisioning, and this should be the primary response. Given that any deviation from this would diminish the benefits of provisioning, such deviations should only come after proof of 'exceptional circumstances', and the ISPs have not provided such proof to date.

[125] However, if some additional measures are found to be necessary, pricing incentives are far more preferable than interfering with traffic. This is because such an approach allows customers to retain a measure of control over their services. A customer that wishes to use more bandwidth in a given month can merely pay for it. In this respect, the impact on users is minimal.

---

[87] See *Infra*, at para. 7.
[88] Reed, above note 2 at para. 22.
[89] For example, provisioning is the best strategy to provide "reliable and affordable telecommunications services of high quality" (s. 7(b)). In addition, provisioning best responds to the "economic and social requirements of users of telecommunications services" (s. 7(h)).
[90] Testimony of Andrew Odlyzko, February 23, 2009, Attachment A, para. XXXXX
[91] 'Exceptional circumstances' was adopted as a minimal threshold that must be met before an ISP may deviate from provisioning as a response to traffic growth in Japan. See *infra*, para. XX (p. 2, Stevenson).

[126] There is also a measure of fairness to pricing incentives, in that the user is getting the bandwidth they are paying for. In addition, such measures are demonstrably capable of meeting current traffic congestion without recourse to more invasive traffic management. Telus, for example, has succeeded in maintaining their network through the use of pricing incentives and provisioning alone.

[127] However, pricing incentives have a number of potentially serious disadvantages if not applied correctly. First, any lack of transparency would negate the fairness involved in pricing incentives, as a customer buying a 5 Mbps line would assume they had access to 5 Mbps of bandwidth, not 5Mbps of traffic for 27 hours.92 Second, pricing incentives should be minimally intrusive. In this respect, peak hour pricing is not sufficiently targeted. It imposes higher fees on low bandwidth customers that are not the primary cause of congestion even at peak hours.93 Excess monthly usage charges are more reasonable in this respect because they target those users that actually produce the most traffic on a network. Third, if not carefully designed, pricing incentives may impact detrimentally on end-users by reducing their level of control over their internet usage. Excess monthly usage charges are also preferable to time of day fees with respect to customer control, because the user is able to ration their usage as needed over a given period of time. Finally, if pricing incentives are used but not measured in a way that is transparent to customers, user will be unable to control their monthly fees. This is potentially a serious disadvantage to consumers. Some ISPs have developed measurement tools and warning systems, but the ideal solution would be a small desktop application that consumers can easily monitor on a regular basis.

[128] Another disadvantage to pricing incentives, one that is more difficult to address, is the lack of control customers have over all aspects of incoming and outgoing data. In any bandwidth connection, the user is always connected to the Internet and so cannot preclude all incoming traffic. It is impossible for a user to control all incoming and outgoing traffic. To some extent, then, users may be charged for traffic they did not choose to generate. This is worse for time of day pricing, as all users may experience uncontrolled traffic during peak periods and incur fees. It also applies, however, to monthly usage pricing, as uncontrolled traffic will contribute to overall monthly bandwidth usage of all users and some users will be charged for such traffic. In addition, any type of pricing mechanism is disadvantageous in so far as it allows ISPs to defer network investment.

[129] Pricing incentives do have some advantages and many of the potential disadvantages of such incentives can be mitigated with careful design. However some disadvantages are

---

[92] This is how long it would take to exhaust Telus' 60 Gb per month allowance if a 5 Mbps line was operating at full capacity.

[93] Testimony of Bill St. Arnaud, February 23, 2009, Attachment C, at para. 47, with respect to peak hours targeting in general.

endemic to pricing mechanisms, and so such measures are only desirable if provisioning alone is demonstrably insufficient.

iii) traffic management and traffic interference

[130] CDM submits that use of any traffic management mechanisms beyond the traditional ones already embedded in the Internet (such as TCP/IP) must be justified.94 Further, based on current traffic growth and reasonable projections into the near future, CDM believes that there is no justification for the use of such measures at this stage. However, it is possible that such measures may become necessary in the future. If and when that time arrives, guidelines must be put in place to ensure that ISPs choose the least intrusive, fairest, and least discriminatory and disruptive measures available. To that end, CDM submits it would be beneficial to adopt Dr. Reed's distinction between 'traffic management' and 'traffic interference'.

[131] Dr. Reed defines traffic interference mechanisms as displaying the following characteristics:

- selectively or arbitrarily restricting traffic associated with certain sources, destinations, content types, applications or protocols;
- base traffic management practices on information not provided by the customer host or application for the purposes of traffic management; and
- do not follow standard mechanisms for signalling congestion.95

[132] Dr. Reed continues to state that "[t]raffic *management* is justifiable in the presence of congestion on the network…Traffic *interference*…is not necessary for ISPs to manage network congestion."96

[133] A number of Canadian ISPs have adopted application-based throttling as their preferred method for addressing congestion. This method can only be classified as traffic interference. It is selective – it directly targets applications such as P2P file-sharing applications. It is not based on information provided by the endpoint for the purpose of routing traffic – it must employ Deep Packet Inspection technology in order to identify the 'application header', an element of the application to which the traffic layer of the internet is generally agnostic. With regards to Dr. Reed's third point, Canadian ISPs that employ this method have not provided details on the precise mechanism used to signal congestion. While it does not appear that any are currently using RST Injection, this type of method should not be permitted.

---

[94] Testimony of Bill St. Arnaud, February 23, 2009, Attachment C, at para. 19.
[95] Testimony of Dr. David Reed, February 23, 2009, Attachment B, at para. 41.
[96] *Ibid*.

[134] In addition to these criteria, Dr. Reed has pointed out that any traffic management procedure employed should make use of IETF approved techniques. Deviating from IETF approved techniques can potentially lead to a form of chaos on the Internet, as each jurisdiction sets up its own methods of managing traffic. This type of chaos would make it very difficult for application developers to develop applications in a predictable way.

[135] Dr. Reed offers a number of IETF approved options that are underutilized and are capable of addressing current congestion issues.

[136] Mr. St. Arnaud, in his testimony, describes a number of disadvantages that apply specifically to application and protocol based throttling. These include:

1. Allowing telcos/cablecos to deploy traffic interference practices such as application specific throttling unnecessarily discourages investment in infrastructure.
2. This practice is not likely to provide an enduring solution to congestion problems.
3. Allowing telecos/cablecos to target whichever applications they wish sets up perverseincentives that can foreseeably lead to discriminatory practices.
4. P2P and file-sharing applications are not the cause of congestion.
5. Allowing telcos/cablecos to throttle P2P and file-sharing application traffic puts ISP resellers, wholesalers and facility leasers at a competitive disadvantage.[97]

[137] Mr. St. Arnaud additionally lists several features that are desirable in an appropriate traffic management approach.[98] One proposal that meets most of Mr. St. Arnaud's points is that made by Comcast. This proposal is based on the following traffic management steps:\

a. Software installed in the Comcast network continuously examines aggregate traffic usage data for individual segments of Comcast's HSI network. If overall upstream or downstream usage on a particular segment of Comcast's HSI network reaches a predetermined level, the software moves on to step two.

b. At step two, the software examines bandwidth usage data for subscribers in the affected network segment to determine which subscribers are using a disproportionate share of the bandwidth. If the software determines that a particular subscriber or subscribers have been the source of high volumes of network traffic during a recent period of minutes, traffic originating from that subscriber or those subscribers temporarily will be assigned a lower priority status.

c. During the time that a subscriber's traffic is assigned the lower priority status, such traffic will not be delayed so long as the network segment is not actually

[97] Testimony of Bill St. Arnaud, February 23, 2009, Attachment C, at para. 20.
[98] *Ibid*. at para. 47.

congested. If, however, the network segment becomes congested, such traffic could be delayed.

d. The subscriber's traffic returns to normal priority status once his or her bandwidth usage drops below a set threshold over a particular time interval.[99]

[138] CDM submits that if any traffic management is necessary, the steps set out in this approach should be the basis of any such traffic management. Preferably, these should be achieved using IETF approved techniques.

Question (3) – Notification Requirements

[139] The Public Notice states, in Q(3):

> *In Telecom Decision 2008-108, the Commission directed Bell Canada to develop and file with the Commission, proposed notification requirements to address future changes that impact materially on the performance of GAS.*

a) Notice of Network Changes – Wholesale Market

[140] The Public Notice asks, in Q(3) a):

> *a) Should these [notification] requirements be extended to other ISPs providing wholesale Internet services such as the third party Internet access services offered by cable ISPs?*

[141] Transparency in network management and pricing are essential to the functioning of the marketplace. Similarly, a level playing field is essential for healthy competition.

[142] Currently, only Bell Canada bears notification requirements with respect to changes that impact network performance. Those notification requirements should be extended to all internet access providers.

b) Notice of Network Changes – Retail Market

[143] The Public Notice asks, in Q(3) b):

> *b) Are similar requirements necessary and appropriate in relation to the provision of retail Internet services?*

---

[99] Comcast, Submissions to FCC, File No. EB-08-IH-1518, WC Docket No. 07-52, September 19, 2008, available online at: <http://www.eff.org/files/Complete%20Comcast%20NM%20Filing%20--%20Date-Stamped%209%2019%202008.pdf>, Appendix B.

[144] Consumers choose among internet service providers on the basis of a number of factors, including traffic management practices. Mandatory disclosure of traffic management practices, across the board, would create a better informed consumer base, and a more competitive and efficient marketplace. Such disclosure is both necessary and appropriate in the retail context.

c) Events Triggering Notice to End Users

[145] The Public Notice asks, in Q(3) c):

> *c) If so, what kinds of practices, and/or changes to practices, should trigger these requirements and what information and how much notice should be provided to end-users?*

[146] Transparency of ISP practices is also fundamental to operation of an efficient and competitive marketplace in Canada for ISP services. Presently, ISP traffic management practices are opaque to consumers and to resellers. This lack of transparency makes it difficult for consumers to compare ISPs on the basis of quality of service. To the extent that such information does seep out into the marketplace, it does so incongruently.

[147] CDM submits that mandated transparency in ISP traffic management practices should not be restricted to disclosures with respect to "kinds of" or "changes to", but rather should also extend to fundamental features of such practices. ISPs must be transparent as to:

a. the technical grounds supporting assertions of congestion, including timely and public disclosure of oversubscription ratios and latency rates; and

b. the nature of traffic management practices in a timely and clear fashion to both wholesale and retail customers, and to prospective customers.

i) Overscription Ratios and Queueing Delay Data

[148] As noted above, ISPs often sell more bandwidth than it can actually provide at any one time. Congestion arises if oversubscription ratios are too high.[100]

[149] ISPs presently treat over-subscription ratios as confidential information. As Bill St. Arnaud states:

> *A significant part of the problem here is that telcos/cablecos are permitted to treat their oversubscription ratios in a manner akin to state secrets. Were telcos/cablecos to publicly advertise that for every 10 Mbps they sell to a consumer, they only provisioned for 1 Mbps at the CPE to CAE leg of the network and even less at various stages between the CAE and Tier 1 routers, they would*

[100] St. Arnaud, *supra* note 3, at para. 8-9.

> *have a hard time justifying their targeting of P2P protocols and file-sharing applications as a tool for reducing traffic. Forcing much needed transparency in oversubscription ratios would make this a competitive issue between telcos/cablecos. Customers could then decide among services based on oversubscription ratios as well as price. Instead of allowing the competitive market to make such decisions, telcos/cablecos are keeping their oversubscription ratios secret and unilaterally deciding to rely on discriminatory Traffic Interference measures such as application-based throttling in lieu of maintaining acceptable oversubscription ratios.*[101]

[150] The introduction of Traffic Interference techniques, in CDM's submission, signals that Canadian ISPs are seeking to maximize oversubscription ratios rather than build capacity.

[151] Customers should be able to inquire as to the oversubscription ration applicable, at any given time, to their service, or to their prospective service.

[152] Transparency with respect to Queueing Delay data also serves to enhance a competitive marketplace for Canadian ISPs. As Dr. Reed states, Queueing Delay is the best metric of congestion.

[153] To the extent that ITEF-compliant traffic management tools are unable to fully address network congestion challenges, Queueing Delay data can support the introduction of more extreme traffic management options.

[154] The ready availability of both oversubscription ratios and Queueing Delay data to consumers permits consumers to make market-based choices among service providers. This creates incentives for ISPs to increase capacity – competing on service – and accordingly enhances the competitiveness of the ISP marketplace.

ii) Traffic Management Practices

[155] ISPs should be compelled to provide much better information to consumers with respect to the nature and impact of their traffic management practices.

[156] Disclosure, to the extent that it occurs, usually occurs in the ISP's "Acceptable Use Policy". However, such disclosure seldom goes to the level of detail that consumers require to make informed decisions about whether or not to purchase services from a particular carrier, or to continue with their current carrier. Far from disclosing their own traffic management practices, carriers impose on consumers a duty to manage their own traffic.

---

[101] *Ibid.* at para. 40.

[157] For example, Rogers' "Terms of Service" requires consumers under the heading "Acceptable Use" to abide by its "policies, rules and limits" (the "Policies"), which are incorporated into the Terms of Service by reference. The Terms of Service reserves Rogers' right to "restrict, change, suspend or terminate" services if the customer's "access, use or connection to the Services, Equipment, or … facilities is impairing or adversely affecting our operation or the use of our Services or facilities by others."[102]

[158] Rogers' "Acceptable Use Policy" similarly prohibits one from using Rogers' services to:

> *(v) restrict, inhibit or interfere with the ability of any person to access, use or enjoy the Internet, the Services or any Equipment used to connect to the Services, or create an unusually large burden on our network, including, without limitation, posting, uploading, transmitting or otherwise making available information or software containing a virus, lock, key, bomb, worm, Trojan horse or other harmful, limiting, destructive or debilitating feature; distributing mass or unsolicited e-mail ("spam"); or otherwise generating levels of traffic sufficient to impede others' ability to send or retrieve information; or to use the Services in an abusive manner in connection with any unlimited packages, options or promotions;*
>
> *(vi) disrupt any backbone network nodes or network service, or otherwise restrict, inhibit, disrupt or impede Rogers' ability to monitor or deliver the Services, Rogers' transmissions or data;*
>
> *(vii) interfere with computer networking or telecommunications service to or from any Internet user, host, provider or network…*[103]

[159] While Rogers admits to blocking ports in its Acceptable Use Policy, it does not admit to engaging in traffic shaping. Indeed, the Rogers.com website lacks any probative disclosure of Rogers' traffic shaping practices – information that is certainly pertinent to many consumers' purchasing decisions.

[160] Rogers disclosure is typical of consumers' experience at most Canadian ISPs. Among Canadian ISPs that we examined, Bell has the most pro-active disclosure of its traffic management practices.[104] That disclosure was mandated by the decision in *CAIP* v. *Bell*. While it provides useful information, it is not prominently located on Bell's website. We could find no direct reference to Bell's traffic management in the "Bell Store" part of Bell's website – where prospective customers would browse Bell's internet service offerings. Such disclosure should be a mandatory part of the purchasing experience.

---

[102] Rogers, Terms of Service <http://www.rogers.com/terms>.
[103] Rogers, Acceptable Use Policy <http://www.your.rogers.com/about/Acceptable_Use_Policy_EN.pdf>.
[104] Bell, Network Management < http://service.sympatico.ca/index.cfm?method=content.view&content_id=12119>.

[161] In our submission, ISPs could and should be profoundly more forthcoming to Canadian consumers with respect to their traffic management practices. Such disclosures should indicate (as applicable):

a. the nature of the practice;

b. the kind of traffic affected;

c. the kind of applications affected;

d. the times of day invoked;

e. port blocking activity;

f. how to secure "unmanaged" services; and

g. the privacy implications of the practice.

Question (4) – "Unjust discrimination": ss. 27(2) of the *Telecommunications Act*

[162] The Public Notice asks, in Q(4) a):

> *a) What, if any Internet traffic management practices employed by ISPs would result in unjust discrimination, undue or unreasonable preference or advantage?*

a) Traffic Interference based on type of application, protocol or user constitutes "unjust discrimination" under s. 27(2) of the Telecommunication Act.

[163] Subsection 27(2) of the Act states:

> *No Canadian carrier shall, in relation to the provision of a telecommunications service or the charging of a rate for it, unjustly discriminate or give an undue or unreasonable preference toward any person, including itself, or subject any person to an undue or unreasonable disadvantage.*

[164] The traffic management measures at issue in this proceeding clearly involve discrimination among subscribers, applications or protocols. They are used to treat certain subscribers of a given service differently from other subscribers of the same service, and certain applications and/or protocols differently from other applications and/or protocols. The question in this proceeding is whether such discrimination is "unjust" under s. 27(2).

[165] There is no set test for determining whether given conduct amounts to "unjust discrimination" or "undue or unreasonable preference" under s. 27(2). Determinations as to whether discrimination is unjust or unreasonable are to be made in light of the public interest[105] as well as the Act and its associated regulations and policies.[106] Intention, although relevant, is not essential to a finding of unjust discrimination; what matters is the effect of the conduct in question.[107]

[166] CDM addressed this issue in its 3 July 2008 submission to the Commission in the matter of *CAIP* v. *Bell Canada*, noting that Bell's throttling of internet traffic violates s. 27(2) on two separate grounds: "First, it results in unjust discrimination and undue disadvantage against users of peer to peer ("P2P") applications. Second, it is an undue disadvantage applied against content providers that use P2P applications to distribute their product." (para.5) CDM adopts the arguments made in that paras. 5-32 of that submission, to the extent that they apply to retail services and to the record in this proceeding.

[167] In addition, CDM submits that the Supreme Court of Canada has provided guidance as to the appropriate test to apply in situations such as the present. In *R.* v. *Oakes*,[108] the Court set forth the test for determining whether *Charter*-infringing conduct was otherwise acceptable by virtue of constituting "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society" under s. 1 of the *Charter*.[109] The Oakes test entails two central criteria:

> *First, the objective must be "of sufficient importance to warrant overriding a constitutionally protected right or freedom"...at a minimum, [it must] relate to concerns which are pressing and substantial in a free and democratic society before it can be characterized as sufficiently important.*
>
> *Second, once a sufficiently significant objective is recognized, then the party invoking s. 1 must show that the means chosen are*

---

[105] *Parardyne Canada Ltd. - Attachment of Subscriber-Provided Terminal Equipment to Dataroute Service,* Telecom Decision CRTC 89-5, Part VII; *Interexchange Competition and Related Resale and Sharing Issues*, Decision 85-19 at p. 73; *Resale and Sharing of Private Line Services*, Telecom Decision CRTC 90-3 at p. 18. See also *Competitive Telecommunications Association et al. - Application to Review and Vary Final Approval of Advantage Canada*, Telecom Decision CRTC 92-4 at p. 15.

[106] *VIARail Canada Inc.* v. *NTA*, [2001] 2 F.C. 25 (F.C.A.) at para. 36; Mandatory Order issued pursuant to subsection 12(2) of the Broadcasting Act against Vidéotron Ltée and its subsidiaries, Broadcasting Decision CRTC 2002-299 at para. 183.

[107] *Mandatory Order issued pursuant to subsection 12(2) of the Broadcasting Act against Vidéotron Ltée and its subsidiaries,* Broadcasting Decision CRTC 2002-299 at para. 183.

[108] [1986] 1 S.C.R. 103; 1986 CanLII 46 (S.C.C.).

[109] *Canadian Charter of Rights and Freedoms*, R.S.C. 1982, c. C-11, s.1.

> *reasonable and demonstrably justified. This involves "a form of proportionality test.*[110]

[168] The Oakes "proportionality test" has three parts:

> *First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right or freedom in question. Third, there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of "sufficient importance".*[111]

[169] This test (sufficiently important objective, rational connection between means and ends, minimal impairment of right or freedom in question, and proportionality between means and ends) can be applied in other contexts where the appropriateness of conduct that impinges on important values or policy goals is at issue.

[170] In the s. 27(2) context "concerns which are pressing and substantial in a free and democratic society" can be translated to "concerns which are pressing and substantial in a free and democratic internet". In this context, the objective is to avoid network congestion and the right or freedom in question is that of users to enjoy unimpeded and non-discriminatory use of telecommunications facilities in accordance with the service package to which they have subscribed. (Note that this test can be applied to Traffic Interference with respect to its impairment of other policy goals such as privacy, competition, and innovation.)

[171] In the context of s. 27(2), the first criteria would require that the objective of relieving network congestion is pressing and substantial. If not, then the discriminatory practices in question should not be permitted. If so, then the second criteria, the proportionality test, must be applied.

[172] In the CDM's submission, network congestion could not be considered "pressing and substantial" unless present standards'-based internet traffic management protocols were not sufficient to fully deal with congestion. ISPs would have to provide objective evidence of congestion and inability to control it with standards-based tools to meet this criterion.

[173] The three-part proportionality test in this situation would be as follows:

---

[110] 1986 CanLII 46 (S.C.C.), paras.69-70.
[111] *Ibid.*, para.70 (emphasis in original).

a. Is the traffic management measure in question designed to relieve, and effective in relieving, congestion on the ISP's network?

b. Does the measure in question discriminate among users, applications, protocols or other content-related aspects of traffic as little as possible, taking into account all other possible approaches to relieving congestion?

c. Are the adverse effects of the measure on users proportional to its effectiveness in relieving congestion?

[174] If any of these questions is answered in the negative, then the traffic management measure in question should be considered to violate s. 27(2). In the following analysis, we apply this test to the facts in this case.

i) Is the objective of relieving network congestion sufficiently pressing and substantial as to warrant discriminatory measures?

[175] In Telecom Decision CRTC 2008-108, the Commission found, on the basis of the record in that proceeding, that "Bell Canada has established that there is congestion in its network during peak periods" and that "intensive use of such applications could, during periods of high internet traffic, result in network congestion and degrade the performance of internet services for other end-users".[112] It thus implicitly found that the objective of relieving network congestion was sufficiently pressing and important as to justify Bell's traffic-shaping measures.

[176] Based solely on the ISPs' responses to Commission interrogatories to date, the problem of network congestion would appear to be sufficiently pressing and substantial as to pass the first part of this test.

[177] However, additional evidence presented in this proceeding by CDM challenges the claim that network congestion is a significant problem likely to continue into the future. As Professor Odlyzko, a widely respected independent expert in internet traffic measurement, states in his testimony:

> *There is no evidence of wireline Internet traffic growing so fast as to require intrusive traffic interference to control it. While there is still vigorous traffic growth, it is at levels that can be accommodated with approximately the current levels of capital expenditure. Just as the computers that we buy provide increased processing power and storage each year for the same price as earlier machines, due to technology progress, telecommunications networks can handle higher levels of traffic each year at the same*

[112] Paras. 29, 30.

> *cost as before. And traffic growth rates have been declining, to levels slower than the rate of improvement of latest transmission equipment.*[113]

[178] CDM therefore questions whether network congestion is as pressing and substantial a concern for Canadian telecommunications as ISPs make it out to be. As Professor Odlyzko points out, network congestion is the result as much of strategic decisions made by ISPs regarding facilities provisioning and service pricing as it is of traffic growth. And objective data on traffic growth – especially forward-looking estimates - do not support the premise on which Traffic Interference rests. In light of the evidence of Professor Odlyzko, the Commission should closely scrutinize ISP claims regarding network congestion before accepting them at face value.

[179] Indeed, as submitted above, it is critical that the Commission establish and implement sound and standard measurements of network congestion (e.g., queuing delay, as recommended by Dr. Reed) that indicate clearly when and where such congestion exists, before accepting ISP claims of network congestion. This information should be made publicly available so that consumers and others can see which ISPs suffer congestion most frequently and/or severely and make purchasing decisions accordingly. CDM submits that if such information is collected and publicly disclosed, a different picture of network congestion may well emerge.

[180] Should the Commission find, despite the evidence and submissions put forward by CDM on this issue, that network congestion is unaddressable by standardized internet protocols and a sufficiently pressing and substantial a concern as to justify Traffic Interference, the next part of the test, involving three sub-parts, must be applied.

ii) Is Traffic Interference designed to relieve, and is it effective in relieving, congestion on the ISP's network?

[181] The various forms of Traffic Interference at issue in this proceeding (most notably throttling based on application, protocol, or user) are purportedly being used to relieve congestion in ISP networks and are apparently doing so somewhat successfully, at least in a micro sense (i.e., looking only at the traffic on a given ISP's network). Thus, they may be seen to pass the first prong of the proportionality test, despite ISP overstatement of the problem.

[182] However, it is worth noting that there may be other, anti-competitive or profit-maximizing, motivations for ISPs to engage in Traffic Interference. Indeed, some Canadian ISPs target their throttling on traffic which, perhaps coincidentally, tends to belong disproportionately to their competitors (e.g., TekSavvy) and/or tends to contain content that competes with

---

[113] Odlyzko, *supra* note 1, at para. 1.

that of their own affiliated content providers (e.g., videos distributed by P2P vs. purchased from Bell's online video store). It may not be pure coincidence, for example, that Telus, which is not as heavily-invested in content production as Bell, does not throttle P2P traffic. More evidence regarding ISP motives for throttling is needed before such speculation can be fairly dismissed.

[183] It is also worth noting, as Bill St. Arnaud does in his testimony, that ISPs have a strong incentive to encourage their users to subscribe to higher-priced services, regardless of capacity, and that this incentive could be a motivating factor behind traffic throttling. At any given DSLAM or cable network stub, there will be different subscribers with different contracted bandwidth rates. When congestion occurs at that node, the ISP may throttle equally or on some basis related to their usage and/or contracted bandwidth. By targeting their throttling on low bandwidth subscribers, ISPs can "upsell" to such customers without increasing capacity. This would clearly be an unjustly discriminatory practice and should not be permitted.

[184] CDM therefore submits that relieving congestion may not be the only motive behind ISP use of Traffic Interference measures, and that any such additional motives are relevant insofar as they conflict with telecommunications policy objectives.

iii) Does the measure in question discriminate among users, applications, protocols or other content-related aspects of traffic as little as possible, taking into account all other possible approaches to relieving congestion?

[185] As set out above under Q.(2)(f) and in the testimony of Bill St.Arnaud and Dr. David Reed, there are many ways in which ISPs can manage traffic so as to avoid congestion. Such practices include:

a. Upgrading networks so as to increase capacity;

b. Pricing based on usage, designed to encourage off-peak use;

c. Various IETF-approved practices, including:

d. Differentiated Service labels (allows the endpoints to specify which packets or flows can tolerate delays or reduced priority for capacity);

e. Queue/packet drops, Early Congestion Notification, and Random Early Drops (signals to endpoints that congestion is imminent which causes them to reduce their usage quickly);

f. Rerouting of flows (rebalances load when alternative paths are available to the destination); and

g. Traffic-smoothing/packet-grooming (vendor-supplied techniques that limit the peak rates of bursty packet flows at an ingress point).

[186] None of these methods of managing network congestion involve discrimination and therefore do not raise issues under s. 27(2) of the Act.114 Thus, they should be exhausted before an ISP resorts to methods that do involve discrimination among users, applications or protocols, in order to manage network congestion.

[187] As long as any non-discriminatory methods of traffic management such as those listed above have not been fully exploited by an ISP, that ISP fails the "minimal impairment" test when it engages in traffic management practices such as application-based or user-based throttling that necessarily involve discrimination among applications or users, and that impede the user experience.

iv) Are the adverse effects of the measure on users proportional to its effectiveness in relieving congestion?

[188] The third prong of the test need not be answered where an ISP has failed one of the two other prongs. CDM submits that this is the case here, as none of the ISPs engaging in discriminatory Traffic Interference have satisfactorily demonstrated their exhaustion of other, non-discriminatory methods of traffic management.

[189] Nevertheless, we submit that the adverse effects of Traffic Interference on users is out of proportion to its effectiveness in relieving congestion, and therefore fails the third prong of the proportionality test.

[190] Throttling of P2P and other traffic has clearly resulted in a significant degradation of service for many internet users. It has significantly diminished the reliability and quality of internet communications for large numbers of users, has not responded to the economic and social requirements of users, and has eroded user privacy, contrary to telecommunications policy objectives as set out in ss.7(b), (h) and (i) of the Act. (see more on policy objectives, below)

[191] Moreover, as noted above under part (a) of the proportionality test, discriminatory traffic-management techniques such as throttling may be used by ISPs to accomplish other, entirely different objectives such as impeding competitors and/or encouraging customers to upgrade to higher-priced services. But even where such motivations cannot be proved, if the effect of traffic management is to disadvantage competitors or to unfairly extract more revenue from low-volume subscribers, such effects, taken together with other direct and

[114] Usage-based pricing involves product differentiation (i.e., different prices for materially different services), not price discrimination (which, in economic terms, means the charging of different prices for the same service).

indirect adverse effects, must be measured against the value of congestion relief achieved by Traffic Interference.

[192] CDM submits that Traffic Interference, regardless of ISP motivations, has had the effect of impeding competition and innovation by targeting a particular application or protocol used by competitors of ISPs to deliver their competing content and by directly or indirectly targeting users who are disproportionately subscribers of competing ISPs. Thus, in addition to its direct adverse effects on users, ISP Traffic Interference has indirectly harmed users by impeding competition and innovation, contrary to the telecommunications policy objectives set out in s.7 of the Act.

[193] In sum, although Traffic Interference may have been effective in relieving network congestion at the individual ISP level, it has been so at a very high price, and without sufficient justification. CDM submits that the cumulative impact of such adverse effects on users vastly outweighs the effectiveness of throttling in relieving network congestion, and therefore fails the third prong of the proportionality test.

b) Conclusion: Application of Proportionality Test to Traffic Interference

[194] For all these reasons, CDM submits that blocking, throttling or otherwise interfering with certain kinds of traffic (*i.e.*, Traffic Interference) for the stated purpose of relieving network congestion unjustly discriminates among applications, protocols, and/or users of internet services contrary to s. 27(2) of the Act.

Question (5) – Prohibitions with respect to "Content": s. 36 of the *Telecommunications Act*

a) Controlling Content, Influencing Meaning or Purpose

[195] The Public Notice asks, in Q(5) a) and b):

> *a) What, if any, Internet traffic management practices employed by ISPs would result in controlling the content, or influencing the meaning or purpose of telecommunications?*
>
> *b) For any Internet traffic management practice identified in (a), what criteria should the Commission apply in determining whether to authorize such practice?*

[196] CDM submits that traffic management practices can constitute control of content and/or influence the meaning and purpose of telecommunications, contrary to s. 36 of the Act. In particular, management practices that stray into Traffic Interference practices can easily violate s. 36.

[197] Section 36 states:

> *Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.*

[198] Section 36 gives statutory force to the principle of common carriage: carriers should not control or influence the content of what they carry. This amounts to a dual prohibition against:

a. controlling the content of telecommunications, and

b. influencing the meaning or purpose of telecommunications.

[199] Applying the ordinary meaning of the words, it is clear that the section 36 prohibition applies to both the purpose and effect of a carrier's practices. In other words, where a carrier's traffic management practices have the effect of controlling content, or the effect of influencing its meaning or purpose, the carrier will fall afoul of the Act. Motives are not a necessary part of the analysis.

[200] The CDM submits that blocking access to specific content would plainly contravene the prohibition of s. 36. Carriers who do so play the role of censor, and attempt to control information communicated. However, most internet traffic management practices are not so blunt. The application-specific throttling common in Canada today, for example, does not block access to content, but rather slows access to content – but the content is still theoretically available.

[201] In our submission, application-specific throttling cannot withstand scrutiny under section 36. The kinds of legitimate content distributed through P2P reflect divisions in the origin of online content. Original content distributed via P2P tends to be independently produced, or lack a mainstream media producer. Mainstream or traditional media, in contrast, tends to use server-centric online distribution mechanisms, or content distribution services such as Akamai Technologies. P2P distribution represents the ultimate disintermediating power of the internet. Using P2P, independent content creators can obtain global distribution without engaging companies that straddle distribution bottlenecks. Traffic management practices that target P2P applications also target such content distributors.

[202] This perspective is born out by the Comments of content organizations in this proceeding. The Documentary Organization of Canada ("DOC") states that:

> *P2P file sharing through BitTorrent is a versatile, cost-effective, and efficient mechanism to distribute independent documentary*

> *film that is currently being employed in varying degrees by Canadian filmmakers.* [115]

[203] DOC goes on to express its concern with application-specific traffic management practices that target BitTorrent:

> *The ISP practice of throttling to manage Internet traffic is a particular concern to the Canadian documentary filmmaking community. DOC supports the notion of Net Neutrality. By employing traffic shaping techniques that target P2P applications, ISPs are effectively taking on the role of gatekeepers. […]*
>
> *The voices and films of independent filmmakers, and of lower-budget emerging and activist filmmakers in particular, are caught in the crossfire of this Internet management practice.*[116]

[204] DOC's submissions with respect to section 36 are particularly compelling:

> *Application-specific throttling practices interfere with and hinder the ability of documentary filmmakers to freely distribute their work. … We note, in addition, that among our members, at least, and within the wider documentary community, it is the independent filmmakers, the emerging filmmakers, the young and the amateur filmmakers who are most likely – although clearly not exclusively – likely to seize on BitTorrent to distribute. Mainstream filmmakers and larger, established filmmakers are likelier to have distribution arrangements that do not require alternative distribution models. Thus, current traffic management practices systematically favour maintstream media while burdening emerging and independent film.*[117]

[205] DOC also identified that the only large ISP in Canada that lacks significant content undertakings is also the only one of them to refrain from application-specific throttling:

> *Many of these ISPs also hold content distribution arms, either cable television undertakings (e.g., Rogers, Shaw) or broadcast undertakings (e.g., Bell). From our own competitive perspective, it is telling that none of the traffic management practices undertaken by these ISPs affect their own content distribution in the slightest.*[118]

---

[115] DOC, Letter to R. Morin re Telecom Notice of Public Consultation and Hearing CRTC 2008-19 (23 February, 2009).
[116] *Ibid*.
[117] *Ibid*.
[118] *Ibid*.

[206] Application-specific traffic management practices are not content neutral. Throttling BitTorrent burdens communications that rely on it. Fundamental economic logic applies: restricting supply has an impact on the market for the throttled communication. Application-specific traffic management practices will result in less of the communications that rely on the application. CDM supports DOC's submission in this regard:

> *Application-specific traffic management practices that target BitTorrent will ultimately result in less content being distributed through that application. To hold otherwise is to assume that those who choose to download our films are not rational. Throttling delays delivery and frustrates viewers. Throttling restricts supply – how can the practice not have any effect on content viewed?*

[207] The CDM observes that DOC's submission is consistent with that of other alternative media points. Miro is an alternative online video distribution platform distributor that utilizes BitTorrent to distribute authorized content. Miro's submissions identifies the anti-competitive undertones of carriers with content undertakings throttling competing content distribution:

> *When traffic shaping practices are employed to limit access to Internet applications (such as P2P) that otherwise compete with the carrier's core business, it undermines fair competition, and consumer choice.* [119]

[208] Miro also identifies the impact that application-specific throttling can have on communications:

> *The effect is that consumers will be dissuaded from using the applications of their choice if such applications are selectively degraded by carriers. Consumers will be forced to use other applications that may not meet their needs as effectively.*[120]

We conclude that carriers employing application-specific content management systems cannot survive a challenge under s. 36 where the application targeted carries authorized communications that are at least partially differentiated from other competing applications. Such practices burden communications with the effect of controlling the content of the communications where the burden is sufficient to dissuade some users from accessing or dissuading some content providers from distributing entirely. Such practices may similarly have the effect of influencing the meaning or purpose of the communications for the same reasons.

---

[119] Miro, Letter to R. Morin re CRTC Telecom PN 2008-19 (23 February, 2009), para. 20.
[120] *Ibid*. at para. 23.

Question (6) – The Policy Objectives of the Telecommunications Act

[209] The Public Notice asks, in Q(6) a):

> *a) What issues do Internet traffic management practices raise concerning the policy objectives of the Act?*

[210] Traffic Interference undermines a number of the telecommunications policy objectives set out in s. 7 of the Act. CDM highlights a few issues below.

a) Undermining the reliability and quality of telecommunications services

[211] Subs. 7(b) establishes the objective of rendering "*reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada*".

[212] Rather than investing in sufficient network capacity to avoid congestion, implementing usage-based pricing to discourage excessive use, or fully exploiting the various non-discriminatory and IETF-approved methods of traffic management, some ISPs have chosen traffic management measures that are explicitly designed to undermine the reliability and quality of some communications, contrary to subs. 7(b).

[213] Some ISPs claim that such measures are needed to maintain overall reliability and quality of telecommunications, arguing that reliability and quality for most users would be undermined if they did not engage in Traffic Interference. But as pointed out above, ISPs are in full control of the reliability and quality of their network; it is their own overselling/under-provisioning that has led to congestion and the consequent undermining of the reliability and quality of telecommunications services.

[214] Throttling of internet traffic by ISPs has had the indisputable effect of undermining the reliability and quality of telecommunications. Indeed, it is explicitly designed to reduce the quality of some communications in order to avoid congestion on the network, and to do so in a manner that is unpredictable and therefore unreliable from the user perspective.

b) Undermining competitiveness of Canadian telecommunications

[215] Subs. 7(c) sets out the objective of "*enhance[ing] the efficiency and competitiveness, at the national and international levels, of Canadian telecommunications*".

[216] By choosing to throttle traffic rather than invest in facilities, some ISPs are undermining the competitiveness of Canadian telecommunications as a whole. As noted in our submissions above with respect to broadband provisioning (see Question (2) f)), Canada's broadband provisioning metrics are falling behind those of other nations.

[217] Moreover, to the extent that ISPs are able to use traffic management techniques to frustrate their competitors, the competitiveness of Canadian telecommunications clearly also suffers.

c) Stifling innovation

[218] Another policy objective, in subs. 7(g), is "*to stimulate research and development in Canada in the field of telecommunications and to encourage innovation in the provision of telecommunications services*".

[219] By throttling emerging new telecommunications protocols such as P2P and file-sharing applications such as BitTorrent, ISPs are clearly stifling innovation in the provision of telecommunications services, directly contrary to subs. 7(g) of the Act.

[220] As CDM stated in its submissions to the CRTC in the matter of *CAIP* v. *Bell*,

[221] P2P applications are an emerging and important form of telecommunications. In fact, their efficiency and adaptability mean that they may become the dominant means of communication in the future. CDM has attached as Appendix 1 a document entitled "Emerging Applications of P2P Technologies" that describes the diverse range of legitimate and licensed content that is distributed via the P2P protocol and which Bell is controlling through its Deep Packet Inspection ("DPI") devices.

[222] As a technology still in its relative infancy, it is unclear what innovative and essential applications P2P protocols may eventually facilitate. Should the Commission countenance Bell's current approach to traffic-shaping, it will effectively place Bell and other incumbent carriers in a position to decide which of the innovative and constantly emerging applications will receive widespread uptake. CDM notes that Bell, in its responses to the Commission's interrogatories, is careful to refer to its "current shaping rules"23 (emphasis added), reserving its prerogative to unilaterally alter once again the flows of internet traffic. Ceding such control to Bell would undermine the unique innovation environment on the internet, a result that is clearly contrary to the statutory policy objective of encouraging innovation in the provision of telecommunications services.

d) Failing to respond to the economic and social requirements of users

[223] It is a policy objective under subs. 7(h) "*to respond to the economic and social requirements of users of telecommunications services*".

[224] Throttling of P2P communications and file-sharing applications clearly fails to respond to the demands of users who are relying on such protocols or applications for economic or social purposes. Especially when there are other non-intrusive methods of dealing with network congestion, and especially when done without full and transparent notice, such

practice not only fails to respond to user needs, but indicates a disturbing disregard for customers.

[225] Even if such throttling is done to protect the economic and social requirements of one class of user, the fact that it frustrates other users makes it inconsistent with this policy objective. Subs. 7(h) is not limited to a certain class of users; it speaks to the needs of all users. Traffic management techniques should be designed so as to respond appropriately to the needs of all users, not just a selected portion.

e) Undermining individual privacy

[226] Subs. 7(i) establishes the final policy objective of "*contribut[ing] to the protection of the privacy of persons*".

[227] One of the most disturbing aspects of certain forms of Traffic Interference (e.g., Deep Packet Inspection) practised by some Canadian ISPs is its privacy-invasiveness. As the recent Heavy Reading Report commissioned by the CRTC, ISP Traffic Management Practices: The State of the Art, states:

> *DPI equipment inspects the contents of packets traveling across an IP network. It can more or less accurately identify the application or protocol in use by examining the source and destination IP address, the port number, and packet payload.*[121]

[228] Many people have expressed concern about the privacy invasiveness of Deep Packet Inspection, especially when used by telecommunications carriers whose business is to carry traffic, not to inspect it. (See, for example, the submission of Christopher Parsons in this proceeding.)

[229] On May 9. 20008, CIPPIC filed a formal Complaint under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") with the Office of the Privacy Commissioner of Canada ("OPCC"), alleging that ISP use of DPI for traffic management purposes constituted a serious privacy invasion, an unlawful collection and/or use of personal information, and a violation of PIPEDA. CDM adopts the submissions made in that Complaint, herein.[122] As of the date of filing this submission, the OPCC has not yet rendered its finding on CIPPIC's Complaint.

[230] Regardless of the OPC's determination of whether Bell et al's use of DPI violates PIPEDA, CDM submits that it clearly does *not* contribute to the protection of the privacy of persons. Indeed, by allowing ISPs to examine the content of traffic on their networks,

---

[121] Heavy Reading, *ISP Traffic Management Practices: The State of the Art* (2009) <http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm > [Heavy Reading].

[122] See http://www.cippic.ca/index.php?page=pipeda-complaints for a link to the CIPPIC Complaint and supplementary filings.

DPI contributes to the *erosion* of user privacy. As long as ISPs are permitted to "open the envelope" and examine any aspect of the content (including application type) of traffic that can be linked to an individual subscriber, they are infringing on user privacy.

[231] As noted in CIPPIC's May submissions to the OPCC, Deep Packet Inspection (as its name suggests) is designed precisely to inspect packets of data at a "deep" level, as contrasted with "shallow packet inspection" commonly used by ISPs to route traffic. It examines Layer 7, the deepest layer of the Open Systems Interconnection model of communications, in order to allow for better identification of underlying applications.[123]

[232] Moreover, DPI permits ISPs to link traffic with particular subscribers so as to engage in subscriber-based traffic management. As the Heavy Reading report states:

> *Technology development and market demand is shifting from applications management to subscriber management. Managing at the subscriber level gives service providers more options, and is linked to emerging concepts such as identity management.*[124]

[233] ISPs have no business examining the content of traffic flowing over their networks except as required by law (e.g., in response to a court order), just as they have no business giving priority to certain communications over others except insofar as one user has paid for a faster service than the other. All exceptions to this well-established rule of common carriage, such as for the purposes of spam containment, should be clearly defined and circumscribed.

[234] Only if it is determined that some form of Traffic Interference is needed in order to achieve a pressing and substantial policy objective, should the Commission even consider permitting ISPs to engage in such activity. And then, the form chosen should pass a proportionality test with respect to privacy invasion, similar to that applied above under subs. 27(2). In particular, the method used should be demonstrated to be effective in relieving congestion; there should be no other, less privacy-intrusive method of achieving that goal; and the privacy-invasiveness of the method should be outweighed by its value in relieving network congestion.

[235] CDM submits that the use by Canadian ISPs of Deep Packet Inspection does not pass this test. DPI, while obviously attractive to some ISPs for their own strategic reasons, is a highly privacy-invasive method of relieving congestion. There are many other, non-privacy-invasive methods that ISPs could instead use for this purpose, including network provisioning, pricing incentives, and IETF-approved technical means of managing traffic (see above).

---

[123] Heavy Reading, *supra* note 121 at p.8.
[124] *Ibid*.

[236] CDM submits that a combination of the above three approaches to traffic management is more than sufficient to avoid congestion on the network and that DPI and similar privacy-invading technologies should therefore not be permitted as traffic management tools. At a minimum, given the privacy-invasiveness of DPI and related technologies, it is incumbent on the CRTC to establish rules that clearly limit ISP use of such technologies in order to protect the privacy of users.

Question (7) – The Policy Direction

a) Implementation of Regulation

[237] The Public Notice asks, in Q(7) a) and b):

> *a) In light of the Policy Direction, address the requirement for, and the appropriateness of, implementing any regulatory measures in relation to Internet traffic management by ISPs.*
>
> *b) For each proposed regulatory measure, comment on how such measure would be consistent with the Policy Direction as well as how these measures could be implemented in the least intrusive manner.*

[238] The Governor in Council has issued an Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives, P.C. 2006-1534, 14 December 2006 (the Policy Direction), which requires the Commission to, among other things:

a. rely on market forces to the maximum extent feasible and when relying on regulation,

b. use measures in a manner that interferes with market forces to the minimum extent necessary to meet the policy objectives, and

c. ensure that non-economic measures are implemented, to the greatest extent possible, in a symmetrical and competitively neutral manner.

[239] The "Policy Direction" requires that the Commission rely on market forces to the maximum extent feasible in order to achieve the telecommunications policy objectives, and when relying on regulation, to use measures in a manner that interferes with market forces to the minimum extent necessary to meet the policy objectives.

[240] In the absence of regulatory action limiting their choice of traffic management approaches and techniques, Canadian ISPs have chosen to engage in practices such as application-based throttling, which CDM refers to as Traffic Interference. As explained above, Traffic Interference by ISPs undermines a number of important telecommunications policy

objectives. Moreover, as also explained above, it violates *Telecom Act* rules against unjust discrimination, undue or unreasonable preference, and influencing the meaning or purpose of telecommunications.

[241] Clearly, reliance on market forces alone has failed to ensure that ISPs use traffic management methods that are consistent with policy objectives. In keeping with the Policy Direction, this is a matter for which some kind of regulation is needed to ensure that policy objectives are met; market forces are insufficient on their own.

[242] Effective regulatory intervention in this case need not interfere significantly with market forces; indeed, it should be designed to facilitate the *effective use of market forces* by ensuring that consumers and others are informed about congestion levels on ISP networks through the public availability of oversubscription ratios and utilization rates based on standardized methodology. As explained by Bill St. Arnaud in his attached testimony, publication of such information will create an incentive for ISPs to invest in network capacity rather than to throttle their customers.

[243] It should also place clear limits on Traffic Interference by ISPs, so as to create incentives for the design and deployment of traffic management technologies that are consistent with telecommunications policy objectives. This has not been the case to date because of the failure of regulators to provide such direction to the marketplace. In the absence of regulatory direction, telecommunications technology designers and service providers have developed and marketed products such as DPI that are inconsistent with policy goals and that have indeed led to a serious erosion of goals including the reliability and quality of telecommunications services, competition, innovation, and user privacy.

[244] Although significant damage has already been sustained as a result of this regulatory failure, it is not too late for the CRTC to step in and provide the signals that the marketplace is not providing and cannot provide on its own.

[245] CDM therefore submits that regulatory intervention is clearly needed in order to ensure that ISP traffic management does not undermine statutory policy objectives, and that such intervention as proposed above would be entirely in keeping with the Policy Direction.

(8) Traffic Management Practices – A Global Perspective

a) Traffic Management Elsewhere

[246] The Public Notice asks, in Q(8) a) and b):

> *a) Discuss any initiatives being examined or undertaken in other jurisdictions in relation to the issues raised in this proceeding concerning the Internet traffic management practices of ISPs.*

b) With respect to any initiatives described in part (a) of this question, discuss their possible applicability in Canada.

[247] CDM has reviewed relevant initiatives and approaches in a number of other jurisdictions. Below is a description of each, after which we discuss the applicability of such approaches in Canada.

i) Japan

[248] Japan, along with Korea, has the fastest internet speeds in the world, and among the lowest prices for bandwidth.[125] Japan has seen a significant increase in internet use over the past several years, driven in large part by fibre to the home (FTTH) deployments.[126] The Japanese government has set a target of 100% penetration of broadband services by 2010.[127]

[249] According to Yasu Taniwaki of the Japanese Ministry of Internal Affairs and Communications, Japan maintains an internet service provider environment that is relatively more competitive than that of North America, due primarily to the opening of Nippon Telegraph and Telephone (NTT) infrastructure to third party DSL resellers in the early-2000s.[128]

[250] As part of its "New Competition Policy Program 2010," the Japanese government has indicated that the internet in Japan should provide "equal access to networks" with "equitable cost distribution [between] networks".[129] Therefore, traffic management practices should allow the network to be accessible to a variety of applications, protocols, and users.

[251] In response to concerns about ISP traffic management practices, in 2007 the government mandated Japan's telecommunication industry and internet service providers to create a set of operational guidelines for traffic management which would be compatible with Japanese law and the government's policies. Four telecommunications carrier organizations -- the Japan internet Providers Association (JAIPA), the Telecommunications Carriers Association (TCA), the Telecom Services Association (TELESA), and the Japan Cable and Telecommunications Association (JCTA) -- established the Study Group on the Guideline

---

[125] Organization for Economic Co-operation and Development, "Price ranges, Mbit/s, Oct. 2007" (2007), <http://www.oecd.org/sti/ict/broadband>.
[126] Hiromichi Shinohar, "Overview of Japanese FTTH Market & Lessons learned from FTTH deployment in NTT" (2007), <http://www.localret.es/localretnews/bandaampla/num18/docs/11num18.pdf> at slide 2.
[127] Ministry of Internal Affairs and Communications (MIC) International Affairs Department, Telecommunications Bureau, "Outline of 2007 Information and Communications in Japan White Paper" (2007, October 12) *Communications News*, 18(13), <http://www.baller.com/pdfs/Japan_MIC_10-12-07.pdf>.
[128] Yasi Taniwaki, "Network Neutrality and Competition Policy in Japan" (2007, December 4) Presentation at the WIK Conference <http://www.soumu.go.jp/joho_tsusin/eng/presentation/pdf/071204_1.pdf> at slide 8.
[129] Taniwaki, "Network Neutrality and Competition Policy in Japan" at slide 18.

for Packet Shaping in September 2007, and published a national ISP "Guideline for Packet Shaping" in May 2008.[130]

[252] The Guideline provides a clear set of prioritized responses to traffic management issues on Japanese networks. The Guideline states that its "basic concept" is that the first response to network congestion should be increasing network capacity.131 Only in "exceptional circumstances" should traffic shaping be used, "where the traffic of a specific heavy user excessively occupies the network bandwidth and consequently degrades the service of general users."[132] The Guideline describes two types of acceptable traffic shaping: restricting the bandwidth, or cancelling the access, of heavy users, and; restricting the bandwidth use of specific network applications.[133]

[253] The exact meanings of "heavy user" and "specific application" are allowed to vary on case-by-case basis, depending on specific ISP capacity. However, the Guideline states that objective data must be used to justify the traffic management; data must show that the quality of service for all users is being degraded by traffic from some users or applications.[134]

[254] The Guideline further states that it is not reasonable to implement packet shaping measures uniformly against all users of a peer-to-peer file sharing software, as it is impossible for the ISP to determine the legality the content distributed.[135] Further, it is also considered inappropriate to completely block the traffic from such applications, as "more moderate" methods of traffic management are available.[136]

[255] The Guideline also indicates that it would be contrary to Japanese law to implement traffic shaping without obtaining clear consent from customers.[137] As a practical matter, users must be informed about their ISP's packet shaping policy in their contract terms and conditions, and agree to them at that time. ISPs are also required to provide relevant information to content providers and other ISPs about any traffic shaping that may impact them.[138] The Guideline states explicitly that traffic shaping must respect individual user

---

[130] Adam Peake, "Presentation to Policy Roundtable 2: Benefiting for convergence, net neutrality & innovation and development" [PowerPoint] (2008, June 16) OECD 2008 Ministerial Meeting on the Future of the Internet Economy, Civil Society-Organized Labour Forum, in Seoul, Korea, <http://thepublicvoice.org/events/seoul08/OECD-Peake.pdf>.
[131] Japan Internet Providers Association, Telecommunications Carriers Association, Telecom Services Association, Japan Cable and Telecommunications Association, *Guideline for Packet Shaping* (2008), <http://www.jaipa.or.jp/other/bandwidth/guidelines_e.pdf>.
[132] *Ibid*., at p. 4.
[133] *Ibid.*
[134] *Ibid*., at pp. 4-5.
[135] *Ibid.*, at p. 4.
[136] *Ibid.*, at p. 9.
[137] *Ibid*., at p. 9.
[138] *Ibid.*, at p. 11.

privacy, therefore making such technologies as deep packet inspection unusable in Japan.[139]

[256] The Guideline allows packet shaping without consent of the user if such network management is "lawfully justifiable,"[140] typically in cases where the integrity of the network from a security standpoint is threatened.

[257] Peer-to-peer technology, while known to be the source of significant traffic management challenges in Japan, is also considered likely to be a key solution for efficient traffic management in the future.[141] Along with sponsoring the development of the Guideline, in 2007 the Japanese Ministry of Internal Affairs and Communications supported the creation of a "P2P Network Experiment Council," made up of content providers, electronics manufacturers, and ISPs.[142] The Council was mandated with the task of studying the use of P2P technologies for the distribution of audio and video content to Japanese consumers.

[258] In 2007, the P2P Network Experiment Council stated that they believed that Japan, despite having among the largest capacity consumer networks in the world, was unlikely to successfully distribute new media content without decentralized distribution.[143] In 2007 and 2008, the Council conducted experiments on P2P content distribution, including the sharing of animation titles from GONZO K.K.[144]

ii) European Union

[259] Cable television has a significantly smaller penetration in Europe than in North America, and most European households lack a "second wire" beyond that originally installed for telephony which could provide high speed internet access to the home.[145] However, competition among European ISPs is generally considered more robust than in North America, as more than 40% of DSL service is provided by third party resellers, although this varies substantially by country.[146] According to Carter et al., real competition exists in this environment only if the wholesale bandwidth provider is prevented from negatively impacting the quality of the service its retail competitors offer to their customers.

---

[139] *Ibid*., at pp. 6-7.
[140] *Ibid.*, at p. 7.
[141] Yasi Taniwaki, "Broadband Competition Policy in Japan" (2008, March), <http://www.too-much.tv/files/080303_bb_policy_in_japaneu.ppt> at slides 29-30.
[142] Ministry of Internal Affairs and Communications (MIC), "P2P Network Experiment Council Symposium to Be Held" (2008, February 1), <http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news080201_1.html>.
[143] *Ibid.*
[144] GDH K.K., "GDH Announces P2P Distribution of Animation Titles" (2007, December 26), <http://www.mania.com/gdh-announces-p2p-distribution-animation-titles_article_85497.html>.
[145] K. Carter, J.S. Marcus, C. Wernick, "Network Neutrality: Implications for Europe" (2008) <http://www.wik.org/content/diskus/diskus_314.pdf> at p. 38.
[146] *Ibid.*

[260] In the past, European telecom regulators emphasized competition as a key mechanism to protect telecommunications and broadband consumers.[147] Regulators believed that if a particular ISP in some way restricted user rights, say to access VoIP or P2P networks, the user would be able to switch to another ISP that did not. Rather than taking a particular stand on what network services should be offered, regulators relied on the market to provide a strong incentive for ISPs to satisfy consumers with varying services.[148] Carter et al. described the 2002 European Union Telecommunications policy framework for ISPs as follows:

> *The current framework explicitly allows operators to offer different services to different customer groups, since price discrimination is perceived as welfare enhancing. It does not allow those who are in a dominant position to discriminate against others in an anticompetitive manner; however, it does not provide [national regulatory agencies] with the means to intervene against operators which are not deemed to have [significant market power] in the event that they discriminate against others.*[149]

[261] In 2006, UK mobile provider T-Mobile launched its Web'n'Walk G3-based mobile internet service, but specifically disallowed the use of voice over IP (VoIP) and instant messaging (IM) over its network.[150] Peter Ingram of UK telecom regulator Ofcom has argued that because customers could switch to other mobile internet offerings that did not have these restrictions, T-Mobile changed its offering to allow such activities, though at an increased price, providing a "market solution" to the matter.[151]

[262] In 2008, the European Commission (the executive branch of European Union) made a series of recommendations concerning ISP traffic management, the majority of which were subsequently endorsed, in principle, by the European Parliament.[152] While recognizing that "legitimate network management practices… and traffic prioritization" can be important drivers of growth and innovation for ISPs, European Commissioner for Information Society and Media Viviane Reding stated in September that anti-competitive behaviour limiting consumer choice should be considered unacceptable.[153] As well, Reding indicated

---

[147] S. Castle, "European telecom regulators emphasized competition" (2008, March 19) <http://www.nytimes.com/2008/03/19/technology/19wireless-web.html>.
[148] Carter et al., *supra* note 145 p. 43.
[149] *Ibid.*
[150] C. Williams, "T-Mobile dumps VoIP restrictions" (2006, September 29) <http://www.theregister.co.uk/2006/09/29/tmobile_voip_tariff>.
[151] P. Ingram, "Should regulators be concerned with net neutrality?" (2006, December 11) Ofcom Communications Research Networks (CRN) <http://www.cambridge-mit.org/object/download/1733/doc/Ingram%20P.pdf>.
[152] V. Reding, *Net Neutrality and Open Networks – Towards a European Approach* (2008, September 30) Speech presented at Network Neutrality - Implications for Innovation and Business Online Conference, Copenhagen, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/473>.
[153] *Ibid.*

that the EU may, in future, impose "minimum quality levels for network transmission services based on technical standards." [154]

[263] These recommendations have been reflected in draft legislation ("the Telecom Package 2009") currently being considered by the European Parliament. The proposed amendments are to the EU Directive 2002/22/EC concerning "universal service and users' rights relating to electronic communications networks." The amendments specific to network management issues are as follows:

> *Recital 16: "A competitive market should ensure that users are able to have the quality of service they require, but in particular cases it may be necessary to ensure that public communications networks attain minimum quality levels so as to prevent degradation of service, the blocking of access and the slowing of traffic over the networks. In particular, the Commission should be able to adopt implementing measures with a view to identifying the quality standards to be used by the national regulatory authorities."*
>
> *Article 22.1: "Member States shall ensure that national regulatory authorities are, after taking account of the views of interested parties, able to require undertakings that provide publicly available electronic communications services networks and/or services to publish comparable, adequate and up-to-date information for end-users on the quality of their services, including and on measures taken to ensure equivalent comparable access for disabled end-users. The information shall, on request, also be supplied to the national regulatory authority in advance of its publication."*
>
> *Article 22.3: "In order to prevent degradation of service and hindering or slowing of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements on undertakings providing public communications networks. The Commission may, having consulted the Authority, adopt technical implementing measures concerning minimum quality of service requirements to be set by the national regulatory authority on undertakings providing public communications networks."*[155]

---

[154] *Ibid.*

[155] Proposal amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks (2009), <http://www.iptegrity.com/pdf/Industry.Coalition.amendments.USD.directive.pdf>.

[264] These amendments, designed to ensure that users' access to particular types of content or applications is not unreasonably restricted, are opposed in their current form by some telecommunications providers.[156] The package also contains directives that subscribers be informed of any change to the provider's traffic management policies. At the time of this writing, the Telecom Package has received second reading in the European Parliament.[157]

[265] In a February 2009 speech before the Lisbon Council, European Commissioner for Information Society and Media, Viviane Reding, stated:

> *New network management techniques allow traffic prioritisation. These tools may be used to guarantee good quality of service but could also be used for anti-competitive practices. The Commission has taken additional steps, through measures proposed to reform our telecom package, to better prevent such unfair abuse to the detriment of consumers.*[158]

[266] Concerns have also been raised about the use of deep packet inspection for traffic by the Article 29 Working Party, which advises the European Union on privacy matters.[159]

iii) United States of America

[267] When compared to Japan and Europe, broadband competition is more limited in the United States, with most markets having, at best, competing DSL and cable-based ISPs. Government measures in the 1990s to force incumbent ISPs to resell access to their infrastructure were only partially successful in expanding competitive offerings.[160] According to the Congressional Research Service, the American ISP market is largely one of ISP duopolies.[161]

[268] In the United States, cable television and telephone infrastructures are regulated differently; the Telecommunications Act of 1996 designated cable as an "information service," while telephone-based internet access services are "telecommunications services."[162] Only telecommunications services are subject to common carrier rules. As a

---

[156] M. Horten, "Harbouring compromises in the Telecoms Package" (2009, February 16), <http://www.iptegrity.com/index.php?option=com_content&task=view&id=255&Itemid=9>.
[157] M. Horten, "IMCO slips a stitch on net neutrality vote" (2009, February 20), <http://www.iptegrity.com/index.php?option=com_content&task=view&id=258&Itemid=9>.
[158] V. Reding, *Freedom of speech: ICT must help, not hinder* V. (2009, February 3) Speech at event on the idea of an EU US Global Online Freedom Act, EP Plenary Session, Strasbourg, <http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/strasbourg-20090203.pdf>.
[159] M. Horten, "Privacy watchdog condemns traffic data amendment" (2009, February 19). <http://www.iptegrity.com/index.php?option=com_content&task=view&id=257&Itemid=9>.
[160] Carter et al., *supra* note 145 pp. 36-37.
[161] C.B. Goldfarb, "Access to Broadband Networks" (2006, June 29) <http://www.ipmall.info/hosted_resources/crs/RL33496_060629.pdf>.
[162] M. Reardon, "FAQ: What is Brand X really about?" (2005, June 27) <http://news.cnet.com/FAQ-What-is-Brand-X-really-about/2100-1034_3-5764187.html>.

result, in 2005 United States Supreme Court ruled that cable companies, unlike telephone providers, were not required by law to resell or share their infrastructure with third party retailers.[163]

[269] However, in August 2005 the Federal Communications Commission (FCC) adopted a Broadband Policy Statement which applied to cable, DSL, and other broadband providers.[164] Although the statement does not have the weight of an enforceable FCC rule, the Commission indicated that it would incorporate the statement into future policymaking. Stating that the "Commission has a duty to preserve and promote the vibrant and open character of the internet as the telecommunications marketplace enters the broadband age,"[165] the FCC adopted the following four principles:

[270] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public internet, consumers are entitled to access the lawful internet content of their choice.

[271] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.

[272] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public internet, consumers are entitled to connect their choice of legal devices that do not harm the network.

[273] To encourage broadband deployment and preserve and promote the open and interconnected nature of the public internet, consumers are entitled to competition among network providers, application and service providers, and content providers.[166]

[274] In a footnote, the FCC offered the qualification that "all of these principles are subject to reasonable network management."[167]

---

[163] T. Glanzer, "Unpacking the Brand X Decision" TMCnews (2005, June 27) <http://www.tmcnet.com/usubmit/2005/jun/1158573.htm>.

[164] Federal Communications Commission, *In the Matters of: Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review – Review of Computer III and ONA Safeguards and Requirements; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; and Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities* [Policy Statement]. CC Docket No. 02-33; CC Docket No. 01-337; CC Docket Nos. 95-20, 98-10; GN Docket No. 00-185; CS Docket No. 02-52 (adopted: August 5, 2005; 20 FCC Rcd at 14988, <http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf>.

[165] *Ibid,* p. 3.

[166] *Ibid.*

[167] *Ibid.*

[275] Rather than drafting rules which reflected the Broadband Policy Statement, the FCC instead transformed it into an enforceable standard through an adjudicatory process involving the largest cable company in the United States, Comcast.

[276] Comcast is the second largest internet service provider in the United States, with over 14.7 million subscribers to its cable internet service.[168] In 2007, several media outlets, including the Associated Press, reported that Comcast had been preventing its subscribers from using peer-to-peer technology to legally share files online.[169] A subsequent investigation by the Electronic Frontier Foundation revealed that Comcast actively interfered with P2P traffic by masquerading as a users' computer and resetting the connection between the Comcast user's computer and the computer of the file recipient.[170] Comcast subscribers had not been informed about this practise.[171]

[277] Comcast initially denied interfering with Bit Torrent traffic, then stated that downloads were not hampered, which though technically accurate was likely misleading. Comcast then stated that P2P traffic was "delayed" rather than blocked, a technical analogy that many considered inaccurate.[172] In November 2007, Comcast vice president of operations and technical support, Mitch Bowling, issued a statement justifying interference with P2P traffic as sound network management:

[278] We have a responsibility to provide all of our customers with a good internet experience and we use the latest technologies to manage our network so that they can continue to enjoy these applications. During periods of heavy peer-to-peer congestion, which can degrade the experience for all customers, we use several network management technologies that, when necessary, enable us to delay—not block—some peer-to-peer traffic.[173]

[279] According to Carter et al., Comcast's network infrastructure was not designed to carry the large volumes of upstream traffic essential to Bit Torrent.[174] The Comcast network used a single router at the cable headend to control transmission in the downstream direction. While this allowed adequate traffic management for downloads, upstream management was much more difficult, as many cable modems, not necessarily under Comcast's control,

---

[168] A. Goldman, "Top 23 U.S. ISPs by Subscriber: Q3 2008" ISP Planet (2008, December 2) <http://www.isp-planet.com/research/rankings/usa.html>.
[169] P. Svensson, "Comcast blocks some Internet traffic: Tests confirm data discrimination by number 2 U.S. service provider" (2007) < http://www.msnbc.msn.com/id/21376597/>.
[170] S. Schoen, "EFF tests agree with AP: Comcast is forging packets to interfere with user traffic" (2007, October 19) <http://www.eff.org/deeplinks/2007/10/eff-tests-agree-ap-comcast-forging-packets-to-interfere>.
[171] Carter et al., *supra* note 145 p. 25.
[172] Carter et al., *supra* note 145 pp. 25-26.
[173] M. Robuck, "Comcast customer sues company for allegedly blocking file sharing" (2007, November 16) <http://www.cedmagazine.com/Comcast-customer-sues-company-for-allegedly-blocking-file-sharing.aspx>.
[174] Carter et al., *supra* note 145 p. 26.

competed for limited bandwidth. Comcast's approach was to reset peer-to-peer connections a set number of times over approximately ten minutes, after which the network would allow the transfer.[175]

[280] In November 2007, media reform organization Free Press filed a complaint with the FCC against Comcast, asking the Commission to rule "that an Internet service provider violates the FCC's Internet Policy Statement when it intentionally degrades a targeted Internet application."[176] Separately, P2P video distributor Vuze filed a petition asking the Commission "to adopt reasonable rules that would prevent the network operators from engaging in practices that discriminate against particular Internet applications, content or technologies."[177]

[281] In the subsequent proceeding, the FCC focused on determining whether the degree to which Comcast's actions were "reasonable network management practices," asking the ISP whether such practices had been "carefully tailored to its interest in easing network congestion."[178] In August 2008, the Commission ruled that the traffic management techniques the ISP had used – resetting TCP connections without regard to network traffic load – were unreasonable. As for alternative and reasonable remedies, the FCC recommended that Comcast use per-user bandwidth caps and fees for high levels of traffic.

[282] The Commission did not rule on Comcast's failure to notify its customers of its traffic management practices. However, it ordered Comcast to disclose to the Commission its network management practices and inform the public of details of its future network management practices.[179]

[283] At this time, the FCC has no detailed rules concerning traffic management. In its Comcast ruling, the FCC announced its intention to deal with future traffic management issues on a case-by-case basis.

[284] While Comcast is currently appealing the FCC ruling,[180] it implemented a set of "protocol-agnostic" traffic management techniques in December 2008.[181] Comcast describes these techniques in its September 19th 2008 compliance filing to the FCC as follows:

---

[175] Carter et al., *supra* note 145 p. 27.
[176] Free Press and Public Knowledge, "Formal Complaint of Free Press and Public Knowledge against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications" (2007, November 1) File No. EB-08-IH-1518.
[177] Vuze, Inc., "Petition to Establish Rules Governing Network Management Practices by Broadband Network Operators of Vuze, Inc." (2007, November 14) *Broadband Industry Practices*. WC Docket No. 07-52.
[178] Carter et al., *supra* note 145 p. 47.
[179] Carter et al., *supra* note 145 p. 48.
[180] O. Malik, "Comcast to Appeal FCC Network Management Order" (2008, September 4), <http://gigaom.com/2008/09/04/comcast-to-appeal-fcc-network-management-order/>.
[181] S. Fisher, "Comcast finalizes its network management strategy" (2008, September 22), <http://www.betanews.com/article/Comcast_finalizes_its_network_management_strategy/1222122139>.

a. Software installed in the Comcast network continuously examines aggregate traffic-usage data for individual segments of Comcast's HSI [high-speed Internet] network. If overall upstream or downstream usage on a particular segment of Comcast's HSI network reaches a predetermined level, the software moves on to step two.

b. At step two, the software examines bandwidth usage data for subscribers in the affected network segment to determine which subscribers are using a disproportionate share of the bandwidth. If the software determines that a particular subscriber or subscribers have been the source of high volumes of network traffic during a recent period of minutes, traffic originating from that subscriber or those subscribers temporarily will be assigned a lower-priority status.

c. During the time a subscriber's traffic is assigned the lower-priority status, such traffic will not be delayed so long as the network segment is not actually congested. If, however, the network segment becomes congested, such traffic could be delayed.

d. The subscriber's traffic returns to normal-priority status once his or her bandwidth usage drops below a set threshold over a particular time interval.[182]

[285] In order to implement these new techniques, Comcast indicated that new congestion management hardware and software would be purchased and deployed near the Regional Network Routers (RNR), sitting between customers' cable modems and Comcast's internet backbone.[183] Comcast also planned to send new software instructions to customers' cable models which would provide for two Quality of Service (QoS) levels for internet access: a "priority" (PBE) level, the default for all users, and a "best effort" (BE) level, which would limit the modem's bandwidth use.[184] Simply put, PBE traffic was to be prioritized over BE, although BE users would still retain network connectivity. In practical terms, Comcast stated that "a user whose traffic is in a BE state during actual congestion may find that a webpage loads sluggishly, a peer-to-peer upload takes somewhat longer to complete, or a VoIP call sounds choppy." [185]

[286] A customer's cable modem would be switched to the BE state only when two conditions were met: the ISP's headend cable modem termination system (CMTS) was at a "near

---

[182] Comcast's Network Management Policy, Attachment B: Description of Planned Network Management Practices to be Deployed Following the Termination of Current Practices (2008) Report to the Federal Communications Commission, <http://www.comcast.net/terms/network> at pp. 2-3.
[183] *Ibid.,* at pp. 3-5.
[184] *Ibid,.* at, p. 6.
[185] *Ibid.,* at p. 13.

congestion state" (as defined by Comcast), and the subscriber was "making a significant contribution to the bandwidth usage on the particular port, as measured over a particular period of time."[186] Bandwidth consumption was to be checked at regular intervals, and if it were to fall below a particular threshold, the modem would be switched from the BE state back to the PBE state.[187]

[287] In its compliance submission to the FCC, Comcast provides detailed information concerning specific hardware and software to be used, system implementation and configuration, the effect of the system on users' broadband experience, and thresholds for determining when a user is in an extended high consumption state, and when a CMTS port is in a near congestion state.

b) Applicability of Foreign Initiatives/Approaches to Canada

[288] Regulatory neglect of internet traffic management in Canada has had a significant adverse effect on Canadian internet users as well as on the health of the Canadian telecommunications network generally. A review of initiatives and approaches in other jurisdictions provides guidance for how to approach this issue in Canada. It is particularly telling that all three jurisdictions that we reviewed, each with quite different traditions of telecommunications legislation and regulation, are arriving at a similar destination, though through quite different routes.

i) Take a Holistic Approach

[289] A particularly informative approach is that of the Japanese government, which conceives of internet traffic management as a component in a broader, multi-year telecommunications strategy. The Ministry of Internal Affairs and Communications sees broadband competition as a key component in consumer choice, and has worked closely with the ISP industry to create a framework for acceptable traffic management. While this is very much in the tradition of Japanese industrial policy, a similar holistic approach in Canada is not out of the question. At the very least, it is incumbent on the Commission to provide, or facilitate the creation of, clear and complete traffic management rules as the Japanese regulator has sought to do.

[290] This is much preferable to the approach of the FCC, which has up to this point indicated that such issues will be dealt with on a case-by-case basis.

ii) Establish Clear Regulatory Rules, not Policy Statements

[291] The U.S. approach also suffers as a result of the lack of clear regulatory authority over internet service providers: the FCC's authority to impose traffic management rules on ISPs

---

[186] *Ibid.,* at pp. 6-8.
[187] *Ibid.,* at pp. 10-11.

is based on a broadly-worded Policy Statement rather than clear legislative authority. In contrast, the CRTC has clear legislative authority under the Telecommunications Act to step in and establish limits, standards, etc. for internet traffic management by Canadian ISPs. It is somewhat ironic that the FCC with its statutory limitations has accomplished more in this respect than has the CRTC. In any case, the CRTC should exercise its legislative mandate and authority by establishing clear, enforceable rules for internet traffic management; it need not limit itself to "policy statements".

iii) Treat Traffic Interference as a Last Resort

[292] In Japan, limiting of bandwidth must only be used in exceptional circumstances, after bandwidth has been increased on the network. Treating Traffic Interference as a last resort is an appropriate approach everywhere, including in Canada. However, the challenge in Canada is to do so in such a way as to minimize interference with market forces. This can be done by creating incentives via regulation that are missing in the marketplace – *i.e.*, creating incentives for ISPs to invest in capacity rather than Traffic Interference in order to handle ever-growing traffic. As argued above, such incentives can be created by a combination of:

a. public disclosure of oversubscription ratios and utilization rates based on standardized measurements; and

b. clear regulatory limits on the types of traffic management practices that are permissible in Canada.

iv) Recognize that Protocol-Agnostic Traffic Management is Possible

[293] The Commission should carefully consider the state of internet traffic management in the United States. The US is an ISP market that, like Canada, has significant geographical challenges and is dominated by cable and telephone ISP duopolies, while arguably subject to a telecommunications regulatory regime which is more resistant to concerns about traffic discrimination then Canada. Nonetheless, the FCC has forcefully applied a reasonableness test to ISP traffic management practices, stating that application-based throttling is "discriminatory and arbitrary" and does not constitute "reasonable network management".188 The application-agnostic practices that have been put into place continue to allow Comcast to manage traffic, while protecting consumers' access to the internet.

---

[188] Federal Communications Commission, *Memorandum Opinion and Order, In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications Broadband Industry Practices Petition of Free Press et al. for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management* (2008, August 20) WC Docket No. 07-52, at page 1.

[294] We believe the Comcast case provides a clear indication that the traffic management techniques used by Bell and other Canadian ISPs are unnecessarily intrusive, inefficient and contrary to both the spirit and the letter of Canadian telecommunications legislation. If Comcast's practices were contrary to US regulation, it is very difficult to image that Bell's similar practices are not a violation of Canadian telecommunications law, which clearly forbids unfair discrimination and undue or unreasonable preferences.

[295] While network management practices vary across Europe, many ISPs, such as the United Kingdom's Virgin Media, engage in application-agnostic management.189 There is no indication from any of these jurisdictions that application-agnostic techniques limit an ISP's ability to adequately manage their network.

v) Do not permit privacy-invasive traffic management techniques such as DPI

[296] It is also clear that the use of deep packet inspection and similar technologies, which may violate privacy laws in many countries, is not necessary to manage internet traffic. The Japanese traffic management guideline clearly forbids the use of DPI, and there is no reason why Canadian ISPs cannot manage traffic successfully without resort to such privacy-invasive Traffic Interference.

vi) Recognize that Throttling Undermines Competition and Choice

[297] Both Japan and Europe emphasize the importance of competition to protecting consumer rights. Choice is severely limited when an upstream ISP throttles traffic for its wholesale customers. In Europe, it appears that ISPs must not only inform their wholesale customers about their traffic management practices, but must provide as close to a "vanilla" service as possible.

vii) Require public disclosure of ISP Congestion and Traffic Management Practices

[298] Broadband customers cannot make informed choices about which ISP will best serve their needs without accurate and complete information concerning the ISP's congestion ratios and traffic management practices. In all three jurisdictions, we found clear and accessible public statements from ISPs detailing their internet traffic management practices. In Japan and the United States, this has been required by regulators. In Europe, we found the practice to be common, and it is likely to required soon by European Union law. The following statements, detailed and written in plain language, are useful examples:

---

[189] Virgin Media Inc., "Virgin Media Broadband: Traffic Management" (2008), <http://allyours.virginmedia.com/html/internet/traffic.html>.

a. Comcast Broadband, Frequently Asked Questions about Network Management: http://help.comcast.net/content/faq/Frequently-Asked-Questions-about-Network-Management

b. Virgin Media, Broadband Traffic Management Statement: http://allyours.virginmedia.com/html/internet/traffic.html

[299] Implicit in this transparency is the necessity for ISPs to provide objective, verifiable data to justify traffic management practices. Again, this is required generally in Japan and to some extent by Comcast in the US. However, the requirements in other jurisdictions may not go far enough: as argued above, Canadian ISPs should be required to disclose publicly their oversubscription ratios as well as utilization rates and queuing delay data based on standardized measurements. Such disclosure will create a powerful incentive for ISPs to invest in capacity and compete on service, to the benefit of all.

viii) Do not demonize P2P technology

[300] Finally, the throttling of peer-to-peer traffic in Canada is out of step with other countries' efforts to utilize P2P for the distribution of content. In addition to mandating the creation of a Guideline for Packet Shaping in 2008, the Japanese Ministry of Internal Affairs and Communication also sponsored a public-private partnership to study the use of peer-to-peer technology for media distribution. Other countries consider peer-to-peer technology to be a legitimate form of media distribution, and it is detrimental to Canadian broadcasters and creators to allow this form of distribution to be crippled.

*** END OF DOCUMENT***