



## Per Vices Corporation

73 Strathcona Avenue

Toronto

Ontario

M4J1G9

Canada

Per Vices Corporation  
73 Strathcona Avenue  
Toronto, Ontario  
M4J 1G9

Mr. Robert Morin,  
Secretary General  
Canadian Radio-television and Telecommunications Commission  
Ottawa, Ontario  
K1A 0N2

2 July 2008

**RE: CRTC File 8622-C51-200805153 - Part VII Application by the Canadian Association of Internet Providers (CAIP) - Application requesting certain orders directing Bell Canada to cease and desist from throttling its wholesale ADSL Access Services.**

Dear Mr. Morin,

We are writing in support of CAIP's letter requesting Bell Canada to cease the selective throttling of wholesale ADSL Access Service. Through the use of Deep Packet Inspection (DPI) technologies, Bell Canada artificially limits the maximum transfer rate available to DSL users whenever they use bandwidth intensive applications not officially recognized by Bell Canada. Per Vices Corporation strongly opposes the actions taken by Bell Canada and submits the following comments for the commission's consideration.

Per Vices Corporation is a company developing innovative technologies based on unconventional and experimental avenues of research. As a small start up, the actions taken by Bell Canada have limited our ability to effectively use our DSL service. In doing so, they have jeopardized the financial viability of our business plan. We do not purchase our internet connectivity from Bell Canada, and unfortunately cannot count ourselves among the majority of end users experiencing an increased level of satisfaction as a result of throttling<sup>1</sup>.

---

<sup>1</sup> 28 MAR 2008 letter sent to Bell Canada ISP customers, "We understand the difficulty this action has caused for you and your customers who are P2P users, but the majority of your end users will experience an increased level of satisfaction".

This letter describes the impact that Bell Canada's Traffic Management Solution (throttling) has had on our ability to effectively use our DSL connection, and the consequences this has on our ability to carry out research, and the commercial viability of our products. We also comment on the mechanism by which Bell Canada uses Deep Packet Inspection (DPI) to throttle users, and discuss the corresponding loss in functionality.

As a small start up, we purchase our DSL service from Tek Savvy Solutions Inc., and are provisioned with up to 5Mb/s<sup>2</sup> service with a 200GB<sup>3</sup> bandwidth cap. Significantly, we ruled out any relationship with Bell Canada's Sympatico branded DSL service because of the throttling limitations imposed upon its users. Prior to March 2008, our historical monthly bandwidth was approximately 160GB total traffic (combined upstream and downstream traffic).

Since Bell Canada started throttling our service, our average monthly bandwidth has dropped significantly. From the beginning of April to the end of June 2008, our average monthly bandwidth usage was 65.79GB. This represents a 59% drop in traffic volume since Bell began throttling our access - a direct result of the artificial cap placed on our connection whenever Bell Canada deems our usage excessive.

Our research depends on the analysis of large files, ranging from 200 MB<sup>4</sup> to over 8 GB. An important step in the commercialization of our product was the design of an efficient mechanism to manage large databases that are accessible to large number of users. As a small company with limited funds, we cannot afford large centralized data centres and dedicated fibre optic internet connections. After considerable research, we decided that a robust distribution network based on peer-to-peer technologies would be the ideal solution.

Instead of concentrating all our data at a single point (effectively concentrating the cost of hosting and serving data to that point), we distribute the data across our user base, spreading the cost over our user base (who pay for their internet connection). Bell Canada's move to throttle peer-to-peer and encrypted traffic has effectively killed the viability of this approach.

Throughout these proceedings, and in response to the CRTC interrogatories, Bell Canada describes, in very general terms, the process by which it uses DPI in throttling. In the third paragraph of its 29 May 2008 letter<sup>5</sup> to the commission, Bell Canada dismisses claims that throttling affects more than peer-to-peer applications;

---

2 1 Megabit per second (Mb/s) is approximately equal to 650 000 bytes/second

3 1 Gigabyte (GB) is approximately 1 000 000 000 bytes.

4 1 Megabyte (MB) is approximately 1 000 000 bytes.

5 "docs-911090-Part VII - Responses to interrogatories - Bell Canada - Attachment 15May08-6.DOC"  
Canada(CRTC)15May08-6 CAIP

*"... there have been several allegations on various websites and in online forums, as well as allegations in CAIP's Application (see in particular paragraph 103), that the Company's Internet traffic management solution is affecting more than P2P applications, such as VoIP and Virtual Private Network (VPN) traffic [...]. However, the Company had investigated several of these reports and in each case had shown that traffic shaping was not the cause of the reported problem."*

In the same letter, they concede that;

*"Therefore, when it comes to using DPI for shaping P2P file sharing traffic, it is important to have the appropriate signatures for the targeted applications configured into the DPI device."*

and;

*"Streaming over HTTP is obviously captured under the HTTP signature since its transfer is specifically on top of HTTP. VPN traffic, on the other hand, is typically encrypted. Therefore, the VPN signatures in the DPI are created leveraging the standard Internet ports. As long as the customer's port setup is correct, VPN traffic will not be shaped. It is noteworthy that most VPN client setups do use the correct standard Internet port."*

We routinely use high grade encryption within our products and in our communications. Bell Canada recognizes that encrypted traffic cannot effectively be analysed by the DPI device. Accordingly, they have associated VPN signatures with the standard ports used by VPN<sup>6</sup>.

The above statements could be perceived as being intentionally vague. Consider a scenario wherein a user runs a VPN over non-standard port, and encounters throttling. In such a case, Bell Canada may consider the problem to be a client configuration error, as they are not running the service over the standard port (despite explicit desire to connect over a non standard port). This seems to be confirmed by Bell Canada's emphasis that so long as the correct port is used, throttling will not occur.

There are several significant flaws with this approach.

The initial decision to throttle traffic by default, unless its signature is specifically recognized by the DPI device employed by Bell Canada, is inelegant and short sighted. Moreover, there does not seem to exist a process by which signatures can be added. And even if such a process existed, it seems ridiculous that people or companies be forced to ask Bell Canada's permission to introduce new protocols and technologies which are not throttled by the DPI device.

---

<sup>6</sup> The standard VPN TCP port is 1723/TCP, with IPSec key exchange protocol using UDP port 500/UDP, and TCP port 50 and 51 for IPSec Encapsulating Security Protocol, and IPSec Authentication Header traffic respectively.

It is important to consider that the IP Security (IPSec) protocols (which can be used to establish a VPN) are transport protocols and are not confined to use in establishing VPN's. In this sense, they are not associated with any specific port, and instead function on an abstraction layer alongside that associated with IP addresses.

A more fundamental flaw in the Traffic Management Solution championed by Bell Canada is revealed when one considers exactly how they dealt with the problem of encrypted traffic. Forced to associate VPN connections with a specific port, they make it trivial for users of peer-to-peer applications to bypass the DPI. A user wishing to download content via BitTorrent needs only to configure their client to use the VPN TCP port to transfer content, associate any remaining UDP ports with the standard IPSec Authentication and Encapsulating UDP ports, and strictly apply protocol encryption to all incoming connections.

This effectively circumvents throttling by the DPI device, at the trivial cost of running an application over an unorthodox port. In contrast, VPN clients using unique ports remain throttled.

Interestingly, Bell Canada also suggests that if we had sufficient funds to afford a dedicated server and internet connection, we could host our database on a web server, and users would be able to download it quickly, without throttling, over the HTTP port 80.

Our design is centred around not requiring users to download the entire database - it would be inefficient for users to download a 10GB database when they only need a small part of it. It makes more sense to distribute the content across large number of users. When a user needs a particular part, they prefer the closest user on the network to download from. This actually has the effect of decreasing overall network utilization when compared to a large centralized database.

As a start-up, we do not have the infrastructure to compete with Bell Canada. We do not have money for dedicated fibre optic connections. And we do not have the patience, influence, or (any) lawyers, necessary to effectively communicate with Bell Canada. We do not purchase bandwidth or internet services from Bell Canada.

We do pay for our Internet access, from an independent ISP, and respectfully request the commission to rule in favour of CAIP's application and allow us to make full use of it, without interference from Bell Canada.

Victor Wollesen  
Chief Executive Officer,  
Per Vices Corporation

Yi Yao  
Chief Technical Officer,  
Per Vices Corporation

CC: Mr. Tom Copeland  
Chair,  
Canadian Association of Internet Providers

Mr. Mirko Bibic  
Chief, Regulatory Affairs,  
Bell Canada