Net Neutrality in Canada and what it means for libraries

Alex Guindon
Political Science subject librarian
Concordia University
Montréal, Québec

Danielle Dennie
Biology, Chemistry & Biochemistry and Physics subject librarian
Concordia University
Montréal, Québec

Keywords

Net Neutrality; Internet Traffic Management Practices; Canada; Telecommunications

Abstract

Net neutrality, the idea that the Internet should be provided to all without discrimination based on content or applications, has been an important policy issue in the last few years. A lack of net neutrality could negatively impact libraries, intellectual freedom, cultural diversity, and the right to privacy. This paper looks at the issues that underline the net neutrality debate and describes how they are shaped by the different actors that are concerned with the future of the Internet. Technological issues, such as traffic shaping by Internet Service Providers, and legal issues in the context of Canada's Telecommunications Act, are also addressed. Finally, the paper reviews the recent CRTC policy on Internet Traffic Management Practices.

Introduction

In recent years, net neutrality has been in the Canadian news. Stories about Bell Canada's discrimination against peer-to-peer (P2P) file sharing, Telus's blocking of access to a union's website and Videotron's CEO, Robert Depatie's pleading for a transmission tariff on Internet content have all contributed to making the issue of net neutrality known beyond a small group of technology pundits and activists. Recognizing the importance of the issue, the CRTC held public hearings in July 2009 on "Internet traffic management practices" in Canada. Although librarians may have a basic understanding of net neutrality, it is often presented by the media as an essentially technical problem and as such may appear daunting to many. The aim of this article is to demystify the issue and, just as importantly, to show how the outcome of the net neutrality debate will impact our work as librarians. The debate will also have bearing on the ability of users and content providers to use the Internet as a tool for education, innovation and communication.

A definition of net neutrality is only just emerging. Some (Ganley and Allgrove 455) prefer to use the expression "access tiering" as a more objective term rooted in technology. However, net neutrality is usually understood as the principle that states that all content transmitted over the Net should be treated equally, regardless of the underlying applications (email, web, FTP, P2P, etc) or the source and destination of the transmission. Tim Wu, the Columbia law scholar who popularized the term net neutrality, provides a more detailed definition in his *Network Neutrality FAQ*:

> Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are *less* specialized -- when they are a platform for multiple uses, present and future (Wu).

There is no doubt about the complexity of the net neutrality debate, but far from being an essentially technical issue, it also touches upon economics, communication, law, and fundamentally begs the question "who controls the Internet?" Much depends upon the answer to that question or at least upon the prevailing philosophy of what social functions the Internet should serve. Should the Net be conceived of as a "common carrier" submitted to public and democratic control, thus serving a public good? Or should it be seen mainly as a commercial venture ruled by the free market or, more accurately, governed by the large telecommunication companies that own the infrastructure?

In an effort to shed some light on these questions, this paper will begin by explaining the main technological and legal issues at stake. We then present a summary of the current debate on net neutrality, followed by an illustration of how traffic management on the Net can have a significant impact on libraries and their users. Finally, we will summarize the recent CRTC hearings and its new policy on *Internet traffic management practices*. Readers who do not have the time or inclination to go through the technical and legal discussions at the beginning of the article should read the short section on *technological aspects* covered next, before skipping ahead to the section of the article dealing with net neutrality and libraries.

Technological aspects

In order to understand net neutrality, it is necessary to first gain basic comprehension of the technical issues at stake. Let's start by defining a few central concepts concerning the original design of the Internet.

All Internet applications --Web, email, P2P, FTP, etc-- work in a similar fashion: the information that is sent and received over the network is broken into small

data packets. Each packet has its own "header" which indicates, among other things, the origin and destination of the transmission and the order in which the packets should be read. The Net was conceived as a simple conduit (also known as a dumb network) devised to transport almost any type of data with little intervention (or computation) done on the network itself. The intelligence of the network rests at its "ends"; it is part of the applications themselves. This is often referred to as the "end-to-end principle" (Ganley and Allgrove 456). The network simply passes data packets from node to node (or router to router) until it reaches its destination. In theory, the source, destination or type of applications are not discriminated against.

Data transmission is based on two principles: FIFO and best-effort. FIFO stands for First-In-First-Out. The first packets received are the first ones to be delivered; the following packets are delivered next in a purely chronological order. The second principle, best-effort, adds conditions to the delivery of packets. It states that there is no guarantee that all packets will be delivered; therefore, some packets may be dropped. For instance, if there is congestion, packets are accumulated in a buffer until they can be transmitted, but if the buffer fills up, the most recently received packets are dropped. All users obtain best-effort service and there is no guarantee as to the bit rate or delivery time ("Best-Effort Service" 136).

These concepts correspond to the original design of the Internet. However, even before the net neutrality debate surfaced, the reality of the Internet was significantly more complicated than was envisioned in the original design. The FIFO and best-effort principles are mitigated by a variety of interconnection, or peering, arrangements between network owners (McTaggart 9-12). Simply put, not all networks or routers talk to each other in an entirely transparent or neutral way. For instance, some Internet Service Providers (ISPs) discriminate against packets whose destination is outside their network[1]. As another example, more recently developed applications are labelled latency-sensitive, such as Voice over Internet Protocol (VoIP) or streaming video, because they do not tolerate delays in the delivery of data packets. Therefore, many network operators, who mostly oppose net neutrality, view the network principles of FIFO and best-effort as design flaws.

Although these examples show that the notion of a purely neutral Internet may have been out of line with reality for some time, these issues did not ignite the net neutrality debate. The controversy only came to the forefront when network owners and Internet Service Providers started using sophisticated techniques like

[1] This is a rather technical matter in which we do not wish to delve in this article. For a complete discussion, see Craig McTaggart. *"Was the Internet ever neutral?". Proceedings of the 34th Telecommunications Policy Research Conference,* September 30, 2006. George Mason University School of Law, Arlington, Virginia, U.S.A. google. Web. July 22, 2009.

Deep Packet Inspection (DPI) to manage traffic and started talking openly about charging additional fees to large content providers like Google or Yahoo. The following section will deal with the various types of infringement to net neutrality principles.

A not so neutral Net

There are several ways for ISPs to manage Internet traffic in discriminatory as well as non-discriminatory ways. Practices are considered discriminatory either because a) they favour some specific content; or b) because they discriminate for or against particular protocols or applications (Longford 15-20). These discriminatory practices have been designated *traffic interference* as opposed to other non-discriminatory techniques that can be labelled *traffic management* (Campaign for Democratic Media 5). Below is a brief description of content and protocol-based traffic interference techniques.

Content discrimination

The bluntest instrument used to discriminate against certain content is to block a specific IP address or address range. Obviously, this amounts to censorship and can be used by governments for political or legal reasons. But it can also be done by ISPs for commercial reasons, as in the Telus case of July 2005. During a labour dispute, the service provider blocked subscriber access to a server hosting a union's web site called "Voices for Change." In so doing, Telus also blocked 766 unrelated web sites hosted on the same server ("Telus"). Although the interruption only lasted a few days, it raised serious questions about censorship and control of information on the Internet by ISPs.

Another traffic interference method that can constitute content discrimination is called *access tiering*. It is the idea that telephone and cable companies that own the network infrastructure (hereafter called *incumbents*) should be free to offer different levels of service (fast lanes and slow lanes) based on the price Internet users pay. As anyone with a broadband subscription knows, this business model is already well established with offerings of high-speed, very high-speed and more extreme high-speed connections; however, and more importantly, what is of concern to net neutrality advocates is that network owners now want to extend that model to content providers. In short, incumbents would like the major content providers to pay a larger amount in order to obtain access to faster lanes. The problem is that smaller firms or non-profits, including many libraries and small educational or cultural organizations, would likely be relegated to a slower lane. As access tiering is more a policy issue than a technological one, we will discuss it further in the section that summarizes the net neutrality debate.

Protocol and application discrimination

The second type of traffic interference deals with the technical capacity for network operators to speed up, slow down or even block certain applications.

Most, if not all, ISPs already use this type of network management to fight viruses or spam. One of the most frequent techniques is called port blocking. It consists of blocking ports generally assigned to certain applications, such as port 25 for the SMTP (Simple Mail Transfer Protocol) application, which is often used by spammers. The problem with this approach is that, beyond blocking spam or illegal file-sharing, it prevents various legitimate uses of email servers or peer-to-peer (P2P) file sharing. Users of P2P applications (BitTorrent for instance) transfer files between computers rather than downloading them from a central server. It is a popular method of exchanging large files --legally or not-- such as movies or music.

Traffic shaping

An even more controversial *traffic interference* method consists of filtering content based on a technique called *Deep Packet Inspection* (DPI). Using DPI, an ISP can "open" data packets to determine their content or the type of applications on which they are based. This goes much further than reading the packet header to acquire information about the source or destination of the data. A good analogy is of the mailman opening a sealed envelope and reading its contents. Needless to say, this practice has raised serious privacy issues. Based on the information acquired through DPI or similar techniques, data packets are then assigned higher or lower priority (or can be blocked altogether) according to the ISP's network management preferences (Riley and Scott 3). The intent is generally to speed up latency-sensitive applications like VoIP or to limit the bandwidth available to P2P. The latter technique (called throttling) is justified by ISPs by claiming that P2P applications require so much bandwidth that they are the main cause of network congestion. As for assigning higher priority to certain applications, network operators contend that this is necessary for the adequate performance of video streaming or VoIP.

Unlike access tiering, which has not yet been implemented at the content provider level, traffic shaping is currently used as a traffic management technique. In fact, companies providing technology such as DPI use the traffic management capacities of the technology as a marketing tool. In 1999, Cisco Systems, a supplier of network equipment, released a white paper explaining how their equipment could be used to give preferential treatment to certain types of traffic flowing across a network (Heskett). Cisco claims:

> For example, if a "push" information service that delivers frequent broadcasts to its subscribers is seen as causing a high amount of undesirable network traffic, you can . . . limit subscriber-access speed to this service. You could restrict the incoming push broadcasts as well as subscribers' outgoing access to the push information site to discourage its use. At the same time, you could promote and offer your own or partner's services with full-speed features to encourage adoption of your services, while increasing network efficiency (Cisco Systems).

Riley and Scott (11) cite other marketing statements by DPI vendors:

- "[Allot] enables quota based service plans that allow providers to meter and control individual use of applications and services"
- "[Allot can] reduce the performance of applications with negative influence on revenues (e.g. competitive VoIP services)."
- "[Camiant's Multimedia Policy Engine is] an intelligent platform for applying operator-defined business rules that determine which customers, tiers and/or applications receive bandwidth priority, at what charge and how much they may use."

As these examples make evident, the use of traffic shaping technology, such as DPI, goes far beyond an effort to create more efficient networks. The unstated rationale behind this new network management approach is likely one of monetization of Internet access which is made possible by a differentiated treatment of data based on the type of applications.

Examples of traffic shaping are numerous. Some ISPs ask consumers or application providers to pay an additional fee for a Quality of Service (QoS) enhancement associated with a specific application. By paying this fee, the user is ensured that priority is given to data packets related to a latency-sensitive application, thus providing a fluid phone conversation or a smooth video streaming experience. As an illustration of this, in May 2005, Shaw Communications , a Canadian cable company and ISP, started implementing a $10 QoS enhancement surcharge to subscribers which ensures reliable access to third party VoIP telephony (for example, Skype). However the surcharge is waived and reliable access is guaranteed for clients who use Shaw's own VoIP product, Shaw's Digital Phone (Shaw).

In December 2005, Rogers Communications admitted to traffic shaping, i.e. bandwidth available for peer-to-peer (P2P) traffic was, and still is, limited on their retail network. In November 2007, Bell Sympatico admitted to using this same technique on its retail network. In March 2008, Bell also started throttling its wholesale customers[2]. When the resellers complained to the CRTC, the issue of net neutrality emerged onto the social and political scene. These are examples of traffic interference that are contrary to the *common carrier* principle described in the next section.

[2] A wholesale network is the portion of it that is leased to competitors (also known as resellers or third party ISPs) who then offer telephone or Internet services to their own customers (Industry Canada 2009).

Net Neutrality and the Law

In Canada and the U.S., net neutrality is supported by telecommunication legislation. The common law notion of *common carriage* is central to the understanding of network discrimination issues. As Wilson (83) explains, traditional common carriers included coachmen, ferrymen and similar professions engaged in the transportation of people or merchandise. The concept was soon extended to railways and later came to include modern telecommunication systems like telegraph and telephone. In essence, common carriers are private companies which, due to their central role in transportation or telecommunications, are vested with some public duties. The traditional obligations of these companies are to offer reasonable rates to all customers, to ensure interconnection between their network and those of competitors and, crucially, to ensure a non-discriminatory treatment of passengers or merchandise transported over their network.

In the past, non-discrimination rules implied that common carriers were prohibited from owning any content that could be distributed through their own network. For instance, "telephone common carriers were forbidden . . . to own newspapers, publishers, broadcasters, or other producers of content" (Wilson 84). These rules have now been abandoned as most telecommunication companies are vertically integrated and simultaneously own newspapers, television stations, and various other producers of content. In addition, recent U.S. rulings (mainly the 2005 BrandX decision by the Supreme Court), have seriously challenged the idea that broadband providers are to be considered common carriers.

In the United States, the Federal Communications Commission (FCC), which is responsible for regulating the telecommunications industry, issued a declaratory ruling in March 2002 defining cable modem services as "information services" under the 1996 Telecommunications Act, as opposed to "telecommunications services" (FCC, "FCC 02-77 Order"). The implication is that information services are not subject to common carrier obligations. This ruling was upheld by the Supreme Court in 2005 in what is known as the BrandX decision. Pursuant to this decision, the FCC adopted a rule which classified all wireline broadband Internet access services, including DSL (the technology used by phone companies to provide high-speed connections) as information services. This meant that all broadband ISP providers were no longer subject to common carrier rules. To mitigate some of the criticisms that were generated by this decision, the FCC released a Policy Statement containing four principles. These have been called the Internet Policy Statement or the Net Neutrality Principles:

- "consumers are entitled to access the lawful Internet content of their choice;

- consumers are entitled to run applications and services of their choice, subject to the needs of law enforcement;
- consumers are entitled to connect their choice of legal devices that do not harm the network;
- consumers are entitled to competition among network providers;" (FCC, "New Principles...")

As of January 2010, the FCC was seeking comments on two additional principles concerning transparency and non-discrimination:

- "a provider of broadband Internet access service must treat lawful content, applications, and services in a nondiscriminatory manner;
- a provider of broadband Internet access service must disclose such information concerning network management and other practices as is reasonably required for users and content, application, and service providers to enjoy the protections specified in this rulemaking" (FCC, "FCC 09-93…")

The FCC wishes to codify these six principles to make them binding rules.

In Canada, there is no distinction between information services and telecommunications services in the Telecommunications Act, therefore, Internet providers must conform to the regulations set out in the Act, including common carriage rules. However, to date the CRTC has generally refused to intervene in the area of Internet retail services ("Telecom Public Notice"). According to the newly issued policy on Internet traffic management practices ("Telecom Regulatory Policy CRTC 2009-657…"), the CRTC now intends to fight discriminatory management on retail networks, but will intervene only after receiving complaints from users. As we will see, subsections 27(2), 7(i) and section 36 of the Act are relevant to net neutrality.

Discrimination and interference with the meaning of messages

Subsection 27(2) of the Telecommunications Act addresses discrimination in telecommunication services, including the Internet. It states that "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" (Telecommunications Act).

Advocates of net neutrality point to the Shaw Quality of Service charge as an example of an unreasonable disadvantage to competitors of VoIP services. They argue that the throttling of P2P traffic by ISPs on their network discriminates

against providers or consumers of legal P2P content. We will elaborate on the effects of this type of discrimination in the section concerning cultural diversity.

Section 36 of the Telecommunications Act deals with possible interferences with the content of messages transmitted via telecommunication networks. It states that "[e]xcept 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" (Telecommunications Act).

When Telus blocked access to its Union website "Voices for Change" it was an extreme example of a Section 36 violation. On the other hand, it has been debated whether the throttling of P2P applications on ISP networks amounts to content control. The Documentary Organization of Canada (DOC) surmises that:

> [a]pplication-specific traffic management practices that target BitTorrent will ultimately result in less content being distributed through that application. . . . Throttling delays delivery and frustrates viewers. Throttling restricts supply -- how can the practice not have any effect on content viewed? (Documentary Organization of Canada).

DOC thus argues that in the case of slowing down P2P files over a network, the control of content is practiced through dissuasion. Slow download (or upload) speeds could discourage Internet users from providing or accessing P2P content. Others also argue that throttling on streaming P2P audio or video, such as music performances or newscasts, can affect the quality of the stream to such an extent that it becomes impossible to watch or listen to.

Privacy issues

According to the Privacy Commissioner of Canada, privacy is a public good and a fundamental human right enshrined in the Charter of Rights and Freedoms and in the Telecommunications Act. Without privacy, freedom of thought, freedom of association, and freedom of speech could not exist (Office of the Privacy Commissioner of Canada, "Telecom Public Notice..."). To address the right to privacy, Section 7 subsection (i) of the Telecommunications Act states that the Telecommunications Act should "contribute to the protection of the privacy of persons" (Telecommunications Act). In addition to this subsection, other legislative measures exist that help protect Canadians' privacy. One of these is the Personal Information Protection and Electronic Documents Act (PIPEDA).

Net neutrality advocates use both of these legislations when addressing the privacy issues that emanate from Deep-Packet Inspection technology. As previously mentioned, DPI devices look deeply into the packets that make up messages or transmissions over the Internet and has been compared to wiretapping. Parsons (12) dubbed it a "massive surveillance technology." and it has also been credited with "enabling third parties to draw inferences about users' personal lives, interests, purchasing habits and other activities . . ." (Office

of the Privacy Commissioner of Canada, "What is Deep Packet Inspection?"). In many countries, DPI equipment has already been used by ISPs to gather information about their customers' Internet habits.

For example, the invasiveness of DPI technology came to light in the United States and England where companies were tracking ISP subscribers' web-browsing behaviour in order to target advertising more effectively. In the USA, a company called NebuAd worked with ISPs to attach devices on their networks that would track page visits, search terms and words on web pages, store this information and provide it to advertisers who could then display targeted ads instead of random ones. Of note is the fact that the device loaded unique identifying cookies onto the subscribers Internet connection which rendered changing computers, browsers, or erasing cookies useless when trying to stop the targeted advertising (Topolski 3).

To date, there is no proof that such invasive practices are being deployed by ISPs in Canada. Nonetheless, in 2008, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a complaint under PIPEDA regarding the "unnecessary and non-consensual collection and use of personal information by Bell Canada and Bell Sympatico through the use of "Deep Packet Inspection" ("DPI") technology" (Canadian Internet Policy and Public Interest Clinic (CIPPIC)). In the Privacy Commissioner's ruling, it was found that when subscribers send information over Bell's network, the DPI equipment monitors these Internet activities by storing subscribers' IP addresses, produced from packet headers, in "flow tables." In its Internet Service Agreement, Bell does inform its customers of possible monitoring, however the Commissioner asked the company to be more transparent in disclosing the ways in which it collects personal information (Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary...").

Net Neutrality timeline in Canada

May 2005	Shaw Communications institutes a $10 Quality of Service (QoS) charge for using third party VoIP services.
July 2005	Telus cuts subscriber access to a pro-union website "Voices for Change."
Dec. 2005	Rogers admits to traffic shaping (aka "throttling") P2P traffic on its network.
Nov. 2007	Bell Sympatico admits to traffic shaping P2P traffic on its retail network.
Mar. 2008	Bell starts traffic shaping P2P traffic on its wholesale network.

Apr. 2008	The Canadian Association of Internet Providers (CAIP) files an application with the CRTC asking it to direct Bell Canada to stop throttling its wholesale Internet service.
May 2008	NDP MP Charlie Angus introduces a net neutrality private member's bill (C-552). The bill dies due to an election in the Fall of 2008.
Nov. 2008	The CRTC denies CAIP's application, allowing Bell to continue throttling its wholesale network.
Nov. 2008	The CRTC announces a consultation on Internet traffic management practices (ITMPs) of Internet service providers.
May 2009	NDP MP Charlie Angus introduces a net neutrality private member's bill (C-398). The bill dies due to the prorogation of Parliament in December 2009.
July 2009	The CRTC holds public hearings on the review of Internet traffic management practices (ITMPs).
Oct. 2009	The CRTC issues a policy (CRTC 2009-657) on ITMPs. The policy provides a framework to assess the discriminatory nature of ITMPs on a case by case basis.

An overview of the debate

The central idea shared by most net neutrality proponents is that the Internet has become an essential public utility, as important, if not more so, than traditional utilities like the telephone, or media such as television or radio. The Internet, being a crucial source of information as well as a major platform for innovation and dissemination of knowledge, should be protected against all forms of discrimination and censorship.

A catalyst for innovation

The Internet as a formidable engine of innovation is arguably one of the strongest points in favour of net neutrality. Several of the major Internet success stories (Google and eBay to name a few) started as very small operations with limited budgets. The underlying idea is that the "dumb network" is extremely conducive to innovation at the system's ends (Longford 39-40).In other words, the open Internet protocols as well as the low cost of market entry create the perfect environment for innovation, especially for individual researchers or entrepreneurs. An additional argument is that innovation is more likely to come from small businesses or start-ups than from large firms already in control of the infrastructure who actually have more incentive to stifle innovation in an effort to protect their business model (Wu and Yoo 581). The argument of the level playing field is also valid when it comes to distribution of information and

research. In a model where anyone, including individuals without significant funding, has easy entry to the Network, it remains possible for non-profit organizations, alternative news sources or smaller research institutions to publish news or research results that can be accessed by a potentially very large number of people. This would become much more difficult in a tiered network environment.

It should be noted that opponents of net neutrality (who call their approach *Net Diversity*) claim that a deregulation (or a tiered network) would foster innovation even more. However, from their perspective, innovation should be facilitated on the network itself, and not at its ends. For example, new specialized conduits should be allowed, such as networks dedicated to video streaming, and traffic management should be improved to speed up latency-sensitive applications and slow-down inappropriate protocols (such as P2P). A related argument maintains that network development, and more precisely that of the last-mile infrastructure, is very costly and the only way that incumbents could finance it is by generating new revenues drawn from access tiering, Quality of Service (QoS) fees and similar methods.

Incumbents' monopoly

The other major argument for net neutrality is related to the nature of the incumbents. The large cable and phone companies are generally in a monopoly or duopoly situation, at least in the North American context[3]. Broadband access sees very little competition since the infrastructure of the network is owned by incumbents, usually one phone company and one cable company in a given territory. Most other ISPs are simply resellers that depend on contractual arrangements with incumbents to obtain access to the network. In *Broadband policy: Beyond privatization, competition and independent regulation*, Larry Press reports that incumbents in the U.S. have been able to successfully lobby against regulations forcing more competition. In many States, they are trying to block projects allowing municipalities to offer local broadband services. As a result, the North American market, or lack thereof, is still largely a duopoly between telephone and cable companies. Recent figures for Canada show that the market share of incumbents in terms of residential Internet subscribers continues to grow while that of third parties is falling:

> . . . over the 2003 to 2007 period, the subscriber based residential market share of the other TSPs (i.e., excluding incumbent TSPs and cable BDUs) declined from 20.7% in 2003 to 7.8% in 2007. The decline in market share is largely explained by the fact that these competitors have a very small

[3] For recent statistics on the competition picture in Canada, see CRTC (2008).

> share of the growing residential high-speed access market (CRTC, "Communications Monitoring Report 2008")[4].

Vertical integration

In the wake of the BrandX decision in the U.S., and the CAIP v. Bell case in Canada (to be discussed below), incumbents appeared to be given the green light to use the network management techniques of their choice, even if those are considered discriminatory by resellers. Given the limited competition, Internet users have few alternatives if they are not satisfied by the service offered by their ISPs. Even more problematic is the fact that incumbents are also content providers; sometimes major media owners. This is an obvious breach of the classic common carrier policy wherein infrastructure providers were strictly prohibited from owning content that could be distributed through their network. The issue at hand is discrimination: there is a clear incentive for incumbents to favour their own content and discriminate against competitors' offerings, as in the example of Shaw Communications's QoS given above.

Another example is that of Bell Canada Enterprises (BCE) which owns Sympatico (their ISP), CTV, several specialty cable channels, and the Globe and Mail newspaper. In its 2007 Annual Report, Bell Canada states that "new unregulated video services and offerings available over high-speed Internet connections are beginning to compete with traditional television services. The continued growth of these services could negatively affect the financial performance of Bell ExpressVu and Bell Canada" (Bell Canada Enterprises).

Considering this statement, it isn't surprising that Bell Sympatico started throttling P2P applications on its retail and wholesale networks in late 2007 and early 2008 respectively. When Bell opened an online Video on Demand service in the spring of 2008, reaction was immediate:

> How can Bell throttle, or shape, Internet traffic while making it easy to sell and download huge media files? (...) [P]utting the brakes on users' downloads, which are more than likely coming from some other source than Bell's Sympatico service, interferes with the way the market operates. The problem is that Bell is making it harder for people to buy movies from other sources while making it easier to buy from Bell (Kapica).

Lack of transparency

The issue of discrimination is compounded by the lack of transparency of ISPs. Until recently, service providers generally published little or no information about the various network management (or traffic interference) techniques that they

---

[4] In CRTC's terminology, TCP stands for *telecommunication service providers* and BDU means *broadcasting distribution undertaking* networks, such as cable and satellite.

used. In these conditions it is hard, or simply impossible for users to know whether their ISP is discriminating against P2P file sharing or throttling VoIP for instance. In the absence of net neutrality *and* transparency, how can one tell if a slow network is the result of "normal" congestion caused by insufficient available bandwidth or of secret network management practices? On a positive note, the new CRTC policy on traffic management (discussed below) stipulates that service providers will now have to disclose any network management techniques on their website, as well as in their marketing documentation and in the terms of customer contracts.

Secretive attitudes by ISPs are not limited to traffic management. ISPs rarely provide precise information about the level of congestion or, conversely, the available bandwidth that they can offer their customers. The current practice is one of "overselling" bandwidth with the view that not all users will make maximal use of their connection at a given moment. While this would be a legitimate practice to maximize network use if done in a transparent and responsible way, the issue is precisely that ISPs keep their oversubscription ratios and utilization rates secret (Campaign for Democratic Media 32-33). In the absence of such information, users cannot make informed choices about their service provider. In some cases, the available bandwidth advertized by an ISP for a specific service may be far from the level of service actually available to the user because of an exaggerated oversubscription ratio. Simply put, the ISP sells more than it can deliver.

Limited investment in infrastructure

The lack of transparency in regard to utilization rate and oversubscription ratios has another negative effect: it limits incentives to invest in network development. Were all ISPs obliged to divulge precise and up to date information about the use of their network, it would foster real competition between incumbents and spur development of the last-mile network where congestion occurs. Instead, in the current situation, service providers are content to use traffic management techniques to deal with congestion. As there is no way for consumers or government agencies to assess the state of the network, there is little pressure on incumbents to make the costly investments (such as fiber optics to the home) necessary to improve the last-mile infrastructure. Some authors go further and argue that incumbents have an incentive to create an artificial scarcity of resource (bandwidth) in order to create additional incentives for their customers to pay for superior packages (extreme high-speed service) or quality of service (QoS) guarantees for VoIP. In the words of Wilson (93):

> . . . incentives may exist for the telcos to arbitrarily discriminate between classes of content (applications) or between service providers in order to create a tiered Internet that is essentially artificial: one that is not grounded in economic fundamentals such as bandwidth scarcity, but rather on the

> broadband carriers' ability to leverage their market power to extract profits under conditions of near-monopoly.

This may be a good short-term business strategy for incumbents but it does not contribute to the development of the network infrastructure, and it appears that Canada is falling behind in terms of broadband penetration and connection speed.[5] Moreover, in the long run the traffic management strategy may turn out to be more costly than investing in infrastructure.

Access tiering

The issue of *access tiering* is another major part of the fight for net neutrality. Most ISPs already charge consumers extra fees for access to a faster or more reliable network. Although some advocates of net neutrality argue that charging consumers more for access to faster "lanes" is an infringement to the neutrality principles, most find it acceptable as long as the ISPs can actually deliver the download and upload rates that they promise. Provided such honest and transparent offers can be achieved, some users' advocacy groups (Campaign for Democratic Media 27) argue that these revenue-generating schemes are preferable to secret traffic interference practices as they allow consumers to have a real choice while providing incumbents with the necessary funds to improve the last-mile network.[6]

On the other hand, the openly expressed intention of some incumbents to start charging extra fees to large content providers for faster or more reliable connections has raised serious concerns in terms of net neutrality. In the wake of the 2005 BrandX decision in the United States, several cable and phone company executives have indicated that they are considering increasing fees charged to big content providers like Google, iTunes or Amazon who are heavy bandwidth users (Longford 28-30). Also targeted would be application providers who offer latency sensitive services like VoIP or video-streaming. The argument of incumbents is that these companies are currently enjoying a "free-ride" as they do not pay adequate access fees for the high level of traffic they are generating.

---

[5] Data supporting this view can be obtained from several recent reports, including the Campaign for Democratic Media (2009) submission to the CRTC; the OECD's Broadband Portal (http://www.oecd.org/document/4/0,3343,en_2649_34225_42800196_1_1_1_1,00.html) ; the 2009 *Global Broadband Quality Study* which is summarized here: http://www.sbs.ox.ac.uk/newsandevents/Documents/Broadband%20Quality%20Study%202009%20Press%20Presentation%20(final).pdf; and the FCC report called *Next Generation Connectivity* (http://www.fcc.gov/stage/pdf/Berkman_Center_Broadband_Study_13Oct09.pdf)

[6] The last-mile is the section of the network that links users' homes or offices to the local switching station of a phone or cable company. Being the smallest component of the network, it is usually where congestion happens. Developing new infrastructure for the last-mile (fibre optics to the home or very high speed wireless technologies like WiMax) is very costly and incumbents claim that new revenue sources are needed, hence their effort to impose a tiered Internet.

BusinessWeek interviewed SBC Communications (later to become AT&T) CEO Ed Whitacre and asked how concerned he was with Internet startups such as Google and Vonage. Whitacre replied:

> How do you think they're going to get to customers? Through a broadband pipe. Cable companies have them. We have them. Now what they would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. So there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using. Why should they be allowed to use my pipes? The Internet can't be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo! or Vonage or anybody to expect to use these pipes [for] free is nuts! (O'Connell).

In answer to this line of reasoning, some authors (Longford 42) point out that incumbents are already counting on large revenues from their corporate customers and that the costs of the network are subsidized by governments in the form of rights-of-way or subsidies to deploy the network in rural communities.

Network providers also contend that the new, latency-sensitive applications demand a different level of service which can only be provided if new revenues are generated. Access tiering as a new business model is a significant departure from the original design of the Internet and threatens to create a tiered network with a fast lane mostly reserved for large and affluent corporations, while smaller firms, non-profits and public entities like libraries could only afford the slower lane. Since incumbents have not yet implemented their vision of a tiered Internet, this issue remains prospective, but it nonetheless holds the potential to completely redefine what the Internet experience is about.

A third way

The respective positions of net neutrality and net diversity proponents are sometimes quite inflexible and do not always recognize valid points made by their adversaries. As Longford (43) remarks, there is another group of people in the net neutrality debate; he has labelled their pragmatic approach the *third way*. Authors like Christian Sandvig, Tim Yu and John Peha, to name a few, recognize the need for some legislation to protect the values associated with a neutral Internet while acknowledging the fact that the Internet in its current form is no longer a purely neutral and transparent conduit for information, and that some traffic management techniques are legitimate and can, under certain circumstances, be beneficial to a majority of users without implying discrimination. Given the existing network management techniques, the emergence of new application classes and the complexity of any legislation to deal with traffic management, it would be impractical and probably impossible to revert to a purely neutral Internet.

The basic idea underlining this *third way* is that some traffic management may be necessary or even beneficial to most users. However, there should be principles (at least) or even legislation (if necessary) to ensure that incumbents do not police their network in discriminatory ways that would favour their interests or be detrimental to their competitors. In that spirit, during the July 2009 CRTC hearings, most of the groups in favour of net neutrality suggested a test for acceptable Internet traffic management practices. Before applying traffic management, ISPs would have to ask themselves the following questions: "(1) Is there evidence of a serious and pressing problem that must be addressed?; (2) Is the solution narrowly targeted at the problem and the least intrusive option?; (3) Does it provide benefits that outweigh any harm it may cause?" (Chung). As we will discuss in the conclusion, the CRTC, in its recent policy on traffic management practices, adopted a *framework* that is very similar to that proposed by these groups.

Although there is no consensus on which forms of traffic control should be permissible, there are a number of principles on which most academics agree. First, traffic management should be based on bandwidth use and *not on application or content discrimination*. ISPs should be allowed to limit individuals' use of the network by imposing daily or monthly caps. Users should be given the choice of how much bandwidth they need, but ISPs should be required to provide a basic broadband service to all users, one which allows all application classes.

Second, ISPs should provide clear justification and notice for all forms of traffic policing that they deploy. There is a need for more transparency, both in terms of traffic management techniques being used and in terms of available bandwidth and oversubscription ratios. Similarly, ISPs should be accountable to independent agencies (like the CRTC in Canada) in regard to their network management practices.

Furthermore, the privacy of users should be protected. Most advocates of the *third way* are against Deep Packet Inspection (DPI). In any case, surveillance activities should abide by legislative requirements (PIPEDA in Canada) and personal information should remain entirely under customer control.

Finally, principles or legislation designed to protect net neutrality should be based on a discussion about the values generally associated with an open and neutral Internet (Sandvig 136). In other words, there is a need for a normative framework which would help legislators or judges differentiate between legitimate traffic management techniques and those contrary to public interest.

Why net neutrality is important to libraries

A commercially minded network, without net neutrality, could negatively impact libraries both as access providers and creators of content on the Internet. Indeed,

without net neutrality, library ideals such as intellectual freedom, freedom of access to information, cultural diversity, and the right to privacy, could suffer.

Intellectual freedom and access to information

Intellectual freedom is a core responsibility and enshrined library value. Most library associations, from the International Federation of Library Associations (IFLA) to the American Library Association (ALA), have statements on intellectual freedom. The Canadian Library Association's statement states:

> All persons in Canada have the fundamental right, as embodied in the nation's Bill of Rights and the Canadian Charter of Rights and Freedoms, to have access to all expressions of knowledge, creativity and intellectual activity, and to express their thoughts publicly (...) *It is the responsibility of libraries to guarantee and facilitate access to all expressions of knowledge and intellectual activity* [emphasis added] (Canadian Library Association).

These ideals of seeking, receiving, sharing and expressing information freely have always been central values to the people involved in developing the Internet ("Declaration of Principles"). Since its inception, the Internet has allowed citizens from different countries with different political or ideological stances to learn from and share information with one another. Around the world, the Internet has been an invaluable tool to fight oppression and dictatorship. By reducing its essence to a crude pecuniary operation, by giving priority access to content guided by commercial interests, ISPs would be overlooking the "necessity for educators, libraries and all citizens to inform themselves and each other just as much as the major commercial and media interests can inform them" ("Network Neutrality").

Without net neutrality, libraries may find it difficult to connect users to the diversity of thought, opinions and information on the Internet. If investment in the public Internet does not keep up with increasing demand, or worse, if the network becomes tiered, content provided by databases or journals from smaller publishers (for example, publishers of open access journals) may become difficult to access as these information providers may not have the means to pay ISPs in order to make their content available on a "fast lane." Library users who encounter slow access speeds when trying to access these resources may turn to commercial websites and services that can provide faster access. These services would most likely come from content providers with substantial financial resources such as Elsevier, Thomson Reuters, or Google.

Internet service providers (ISPs) having control over Internet content or the way in which it is accessed has an impact on other issues that are of concern to libraries, such as copyright. For example, by blocking certain applications like P2P file sharing, ISPs can indirectly affect fair dealing provisions set out in copyright laws. Frieden (673) argues that if ISPs are in a position to decide which content or application should be degraded or blocked, they would be making a priori judgments as to what constitutes fair dealing. This removes the ability of

individuals to decide for themselves what content can be used under these provisions and effectively transforms the network into a proxy censor and repressor of fair dealing.

The reduction of information diversity through content tiering or blocking would also negatively affect librarians' ability to teach independent, critical thinking skills, an important information literacy competency. These skills are at the core of innovation and knowledge production. The ability to access and critically evaluate all forms of information is a precondition to participation in political and socio-economic activities. Knowledge production and innovation underpin the post-industrial economies of most Western nations, and libraries play a key role in fostering scientific progress. Letting ISPs decide which applications and which content obtain priority access may well stifle knowledge growth and innovation.

Slower scientific progress would not only affect our economies, but also libraries' ability to use emergent technologies in the provision of services. LOCKSS (Lots of Copies Keeps Stuff Safe) is a good example of such innovative technology. It consists of a P2P application that allows libraries to archive and preserve authorized online content from publications to which they subscribe. If a journal publisher's website becomes inaccessible, its content will still be available at the library thanks to LOCKSS. LOCKSS may not have been possible if innovation on the Internet was kept in check by ISPs. Without net neutrality regulations, other applications could be blocked or throttled which could make videos, audio, images, or datasets difficult to access or share. However the future of content provision unfolds, libraries or publishers should have the flexibility to use the applications which best serve their educational or research base.

Although libraries' most prominent role is to act as a gateway to a diversity of resources, they also act as content providers by collecting and organizing quality, non-commercial information. For instance, libraries provide access to print or audio-visual collections in online digital collections and institutional repositories (which may contain the research output of an educational institution). As content providers, libraries would not be able to compete in the context of a two-tiered Internet:

> [I]t is unreasonable to think that (...) libraries would be able to pay an additional premium (besides what they already pay for hosting and bandwidth) to ensure that users can access their sites quickly. Sites created by libraries and other nonprofit institutions would quickly lose the competition for "eyes" if they were forced to compete with sites produced by companies who can afford to cut deals with ISPs for premium service (Bridges).

Net neutrality on campus

In a knowledge society, libraries should play a proactive role in network provision at their institutions. Unfortunately, few libraries have significant input into the

university's network operations. As it stands, due to restrictive network management practices both on campus and on retail ISP networks, many libraries may not have the potential to experiment with content delivery through different applications, such as BitTorrent. Sadly, the network management policies of many universities explicitly forbid P2P applications (IITS; de Beers). For instance, Skype, a P2P VoIP provider that can be used to offer virtual reference, is not a viable option for many libraries as it is often blocked or throttled, either by the university itself or by users' ISPs. Were ISPs or campus network providers to target other types of applications, such as streaming video or audio, offering online learning through these media would prove challenging. Also of note, some universities already block websites, such as Facebook and MySpace, which, in addition to their well known social networking functionalities, can be used as communication tools by faculty and librarians.

Usage caps, i.e. setting a limit on the amount of data that an individual can download, are another concern in academia. Although not everyone agrees that this practice is, strictly speaking, a net neutrality concern, it can have an impact on research activities. At the University of Toronto, students have usage caps on their wireless access: although the stated goal of the wireless service policy is to support "students' academic activities," it also states that heavy downloading or uploading of data could lead to potential disconnection from the University network (University of Toronto Scarborough). Even if the IT department's only concern is to maintain optimal network performance, disconnecting users from the Internet could seriously impact research and academic activities in a research setting where large datasets or image files are stored in online repositories. At its worst, if university IT departments introduce data caps as a way to police their networks, then disconnecting users goes against the presumption of innocence. Heavy downloading does not a priori entail illegal activities such as copyright violations through music or file sharing. Traffic policing on academic campuses is not only a theoretical possibility. In the United States, the Higher Education Opportunity Act (reauthorized in 2008) contains new provisions that direct universities to implement traffic filtering technologies making them common practice on American university campuses.

This is only one type of breach of net neutrality and advocates in the field of higher education also fear the prospect of a tiered Internet, which would raise the costs of a college education. Unlike private universities with better funding, smaller colleges and universities are concerned that the only way to afford access to a faster network would be to increase tuition fees.

As mentioned earlier, net neutrality advocates have pointed out that investing in broadband infrastructure, instead of throttling bandwidth, would be highly beneficial. This is especially true for education and research. In fact, the Internet2 network (http://www.internet2.edu/), which connects several American universities, government, and research organizations to a very fast broadband network, provides compelling examples of the benefits of greater broadband

speeds to research and education. These include data mining on large datasets, controlling high-tech microscopes remotely, and collaborating with researchers at the Large Hadron Collider in Switzerland (Atkinson, Ezell, Castro, and Ou, 26). Atkinson, *et al.* (27) contend that bandwidth limitations on retail ISPs in North America are preventing the widespread emergence of Internet2 applications, whereas Asian countries, such as Japan, already have the bandwidth capacity to easily deploy these innovations.

In their research, Corbató and Teitelbaum, managers for the Internet2, found that an overabundance of bandwidth was a simpler and more economical way of maintaining a high speed network, rather than using technological means to control congestion. Unfortunately, in some circles, such as the cultural sector, limited bandwidth and DPI technologies are already having an effect on innovation.

Cultural diversity

Canada was the first country to sign the UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions, which was ratified in 2006. According to the Canadian Heritage website, Canada has been highly supportive of the Convention whose goals are to "protect and promote the diversity of cultural expressions" and "to create the conditions for cultures to flourish and to freely interact in a mutually beneficial manner." Interestingly the Convention affirms that cultural diversity is:

> made manifest not only through the varied ways in which the cultural heritage of humanity is expressed, augmented and transmitted through the variety of cultural expressions, but also through diverse modes of artistic creation, production, dissemination, distribution and enjoyment, *whatever the means and technologies used [emphasis added] (UNESCO).*

By clearly advocating for net neutrality, the spirit of the Convention and the importance of cultural diversity were largely supported by a variety of cultural groups during the CRTC *new media hearings* in February 2009 and in submissions to the CRTC *Internet traffic management practices hearings* of July 2009. These groups include the Canadian Film and Television Production Association, the Documentary Organization of Canada, the Songwriters Association of Canada, and the Independent Media Arts Alliance, to name just a few.

Of particular note, the Documentary Organization of Canada (DOC) had this to say about the ISP practice of application-specific traffic management (i.e. throttling of P2P applications):

> BitTorrent has developed into an efficient and effective mechanism to distribute large content files lawfully. Many documentary filmmakers now routinely use BitTorrent: 1) as the sole or primary method to distribute their

> films; and 2) as part of a multi-distribution strategy to reach as broad an audience as possible -- legally, openly and purposefully. Throttling of file sharing applications slows down file transfer speeds (...) and (...) can make it virtually impossible to transfer files through such applications (...). Documentary filmmakers typically work with very limited resources in order to make films that contribute to the Canadian cultural landscape and marketplace of ideas. BitTorrent makes it affordable to distribute high quality digital video and enables filmmakers, especially smaller, emerging filmmakers with constrained budgets, to contribute to that marketplace. (...) ISPs are not in an economic position to be immediately sensitive to the perspective of the independent Canadian documentary film community. They generally do not operate with a global outlook mindful of the perspective of independent voices that view the Internet as an open and democratic medium for communication, and who rely on it in part for their economic and professional livelihood. DOC thus believes that ISPs are in an unsuitable place to make decisions regarding Internet content (Documentary Organization of Canada).

There are other providers of cultural or informational content that have started using P2P applications. For example, the CBC distributed the TV programme Canada's Next Great Prime Minister through BitTorrent (Cheng 2008). A multimedia series created by the Globe and Mail and entitled "Download Decade" was also made available through torrent download ("Download Decade" 2009). Some public broadcasters go much further: Norway's NRK started distributing *all* of its programming via BitTorrent in early 2008 (Anderson).

Net neutrality can ensure that libraries, museums, and other not for profit organizations continue to provide access to a diversity of cultural content, no matter how this content is distributed.

Recent development: Public hearings and a new policy on Internet traffic management practices

As previously mentioned, when Bell started throttling its wholesale network in March 2008, the resellers complained to the CRTC, which initiated prominent public debate on the issue of net neutrality. In April 2008, the Canadian Association of Internet Providers (CAIP), Canada's largest ISP association, filed an application with the CRTC asking it to direct Bell Canada to stop throttling its wholesale Internet service. Many organizations and companies and hundreds of individuals sent letters to the CRTC in support of CAIP's application (CRTC, "2008-04-03...").

In November 2008, the CRTC issued its ruling in the CAIP v. Bell case, denying CAIP's application. The CRTC sided with Bell on most key issues and thus allowed throttling to continue on the wholesale network (CRTC, "Telecom Decision CRTC 2008-108..."). This decision surprised many observers since

three months prior to the ruling, a similar case in the United States elicited an opposite reaction from the FCC. In August 2008, the FCC relied on its net neutrality principles to rule against Comcast, an ISP that was using DPI equipment to throttle P2P applications on its network. The ruling forced Comcast to apply protocol agnostic traffic management and affirmed the following:

> The record leaves no doubt that Comcast's network management practices discriminate among applications and protocols rather than treating all equally (...) [I]n laymen's terms, Comcast opens its customers' mail because it wants to deliver mail not based on the address or type of stamp on the envelope but on the type of letter contained therein (FCC, "FCC 08-183 Order").

Despite the CRTC's ruling in favour of Bell Canada, the Commission was sensitive to the fact that many filings from a variety of net neutrality advocates had been submitted for this case. It therefore decided to hold a consultation and hearing entitled *Review of the Internet traffic management practices of Internet service providers* (CRTC, "Telecom Public Notice CRTC 2008-19...") in July 2009. The consultation elicited 500 comments and over 13,000 online submissions (CRTC, "Telecom Regulatory Policy CRTC 2009-657..."). There were 29 presentations by a diversity of participants ranging from consumer groups to ISPs. Issues discussed included frameworks for determining acceptable Internet traffic management practices (ITMPs), transparency of traffic management practices, and privacy. In October 2009, the Commission issued its new policy on the issue. Let's examine the key elements of the policy.

With regards to Subsection 27(2) of the Telecommunications Act which states that carriers shall not discriminate against certain applications or protocols, the CRTC agrees that some traffic management practices can affect innovation and performance of the network. The policy also recognizes that investment in building the network is the best tool for dealing with network congestion. Furthermore, economic measures, such as data caps or discounts for Internet use during off-peak hours, are considered preferable to technical measures for traffic management.

That being said, the CRTC agrees with ISPs that traffic management may be necessary in certain conditions. A framework was therefore established to enable the CRTC to evaluate whether a particular ITMP complies with subsection 27(2). According to the policy (CRTC, "Telecom Regulatory Policy CRTC 2009-657..."), when answering a complaint, the ISPs will need to describe the ITMP being employed, as well as the need for it, its purpose and effect. In addition, in the case of an ITMP considered discriminatory, the ISP will need to:

- "demonstrate that the ITMP is designed to address the need and achieve the purpose and effect in question, and nothing else;

- establish that the ITMP results in discrimination or preference as little as reasonably possible;
- demonstrate that any harm to a secondary ISP, end-user, or any other person is as little as reasonably possible; and
- explain why, in the case of a technical ITMP, network investment or economic approaches alone would not reasonably address the need and effectively achieve the same purpose as the ITMP" (CRTC, "Telecom Regulatory Policy CRTC 2009-657...").

Some net neutrality advocates are disappointed that the CRTC did not define the Internet as a public good; such recognition would require ISPs to comply with common carriage provisions. Instead, the CRTC ruled that ISPs may continue to apply traffic management practices which they feel are appropriate to retail Internet services, without any requirement for prior approval from the Commission (CRTC, "Telecom Regulatory Policy CRTC 2009-657..."). Others see the establishment of a framework to contain traffic management as a step forward with the only downside being its enforcement. However, the Commission decided to establish a complaints-based regulatory approach in order to look into inappropriate practices by ISPs. This approach puts the burden of proof on users.

This complaints- based process may not provide enough protection for Internet users. For example, in May 2009, the Canadian Association of Internet Providers (CAIP) and other consumer groups filed an application with the CRTC to review the November 2008 decision which allowed Bell to continue throttling its wholesale network. One week after the traffic management policy was issued in October 2009, the CRTC addressed CAIP's application as their first consumer complaint.

Among the issues brought up in their application, CAIP reaffirmed that throttling was an infringement of Section 36 of the Telecommunications Act. Furthermore, CAIP challenged the facts that Bell Canada put forward to claim that it only throttles non-time-sensitive P2P file-sharing applications. Nonetheless, the CRTC ruled that it received no evidence to prove Bell wrong regarding non-time-sensitive P2P applications, and therefore decided to maintain its original decision allowing Bell to pursue throttling of its wholesale network (CRTC, "Telecom Decision CRTC 2009-677..."). Therefore, in its first consumer complaint decision, the CRTC has sided with the Internet Service Provider.

To address the issue of transparency, the Commission ruled that any traffic management measures applied by ISPs should be disclosed to their customers. For example, traffic management practices will need to be posted on their website and should include the reasons why ITMPs are applied, who and what

type of traffic is affected by them, when they occur, and how speed or other Internet experiences might be affected.

The policy also addresses privacy concerns based on PIPEDA and subsection 7(i) of the Telecommunications Act. Although many ISPs argued that PIPEDA was sufficient to address privacy issues that arise through the use of Deep Packet Inspection (DPI) equipment, the Commission considered it appropriate to "impose a higher standard than that available under PIPEDA in order to provide a higher degree of privacy protection for customers of telecommunications services" (CRTC, "Telecom Regulatory Policy CRTC 2009-657...").In light of this, the Commission forbade ISPs from disclosing personal information or using it for purposes other than traffic management.

Finally, the policy looks at the issues of content control (Section 36 of the Telecommunications Act). The Commission agreed with many consumer advocacy groups by stating that noticeable degradation of time-sensitive traffic (for example streaming video or VoIP) "amounts to controlling the content and influencing the meaning and purpose of the telecommunications in question" (CRTC, "Telecom Regulatory Policy CRTC 2009-657...") and should therefore not be permissible without prior approval by the CRTC. However, with respect to non-time-sensitive traffic, the Commission found that delays in downloading P2P content, for example, cannot be considered an offence unless the speed is so slow that the content can essentially be considered blocked.

Conclusion

The CRTC policy is a step in the right direction. For the first time in Canadian history, there is a framework that prescribes limits to Internet traffic management practices (ITMPs). The principles adopted are in line with ideas put forward by the proponents of the *third way* to deal with net neutrality issues. In short, while recognizing that in certain circumstances there may be a need to apply technical control measures to Internet traffic, the CRTC stresses the importance of creating as little interference as possible and of avoiding discriminatory techniques. But there remain serious doubts about the practicality of these rules since the burden of proof falls on the citizens and Internet users' associations. In light of the size of the companies owning the infrastructure and of the significant legal and technological resources at their disposal, it is hard to see this as a fair solution.

Librarians and other citizens concerned with the development of the Internet in Canada should be aware of what the CRTC decision *does not* address. The mandate of the review as reflected in the new policy is fairly narrow: it is essentially limited to technical considerations on Internet traffic management. While it touches upon the further development of the Internet infrastructure in Canada, this is only a peripheral concern. It certainly doesn't question the lack of competition in the Canadian broadband "market" or the fact that Canada is falling

behind other OECD countries in broadband penetration and speed of connection. Not surprisingly, the CRTC policy remains firmly rooted in a market-based approach (even in the absence of such a market) and tries to avoid what it sees as unnecessary legislation of the Internet. There is something to be said for a moderate approach to such a complicated question. What is missing in the CRTC policy is a vision of what the Internet represents for a modern and democratic society and how such a crucial network should be governed.

To be fair, given the nature of the CRTC as a regulatory agency, these criticisms pertain to topics likely beyond its mandate. A political will is needed to address those difficult issues. The Internet has become an unprecedented conduit for information and the dissemination of knowledge, as well as a tremendous platform for technological innovation. In light of the Internet's role in so many facets of life, it should be considered an essential public utility and be treated as such. Difficulties related to the slow development of the last-mile infrastructure -- which is a significant element to explain network congestion -- and the lack of competition will not go away. These challenges will need to be addressed with an open mind and new solutions, such as municipal ownership of local infrastructure or the development of very high-speed wireless networks. On the other hand, if the current duopoly situation is to persist, then, at the very least, the common carrier status of the incumbents has to be reaffirmed. In any scenario, the Canadian government should play a leadership role in the development of the infrastructure and should ensure that the Internet remains an open network where the free dissemination of information prevails over commercial considerations.

Glossary

Common carrier

In common law, traditional common carriers were transportation companies (railways, ferries, etc) that, because of their importance in providing essential public services, were under obligation to offer a non-discriminatory service (transport any person or good under the same conditions) and to offer reasonable rates. These legal duties were later extended to telecommunication companies including telephone and Internet providers. In the United States, since the BrandX decision by the Supreme Court in 2005, Internet providers are no longer considered common carriers.

Best effort

Data transmission principle according to which there is no guarantee about the bit rate or delivery time of information sent over a network. Additionally, in case of network congestion, some information (data packets) may be dropped.

Incumbents

Companies that own the local Internet infrastructure. In North America, incumbents are generally telephone or cable companies and most enjoy a local monopoly or duopoly over the network.

ISP (Internet Service Provider)

Companies that offer Internet access to individuals or businesses. ISPs either own part of the local Internet infrastructure (in this paper, we identify those as *incumbents*) or are resellers that have contractual arrangements with network owners.

ITMP (Internet Traffic Management Practices)

Term used by the CRTC to designate any technical method used by Internet Service Providers (ISPs) to control (block, slow-down or prioritize) Internet traffic on their network. These techniques can include both content-based and application-based manipulation of traffic.

FIFO (First-In-First-Out)

Data transmission principle according to which the first information received (data packets on the Internet) is the first transmitted. Packets are thus transmitted in chronological order.

P2P (Peer-to-Peer)

Denotes a communication protocol based on several computers that communicate together without the need for central coordination (a server), in

order to share files. BitTorrent is one of the most well known P2P protocols. In the last 10 years, applications which popularized file-sharing include Napster (defunct since 2001), Kazaa (now a subscription service) and Vuze.

Throttling

A type of traffic interference technique that aims at slowing down certain applications, most frequently peer-to-peer traffic.

Traffic interference

Discriminatory traffic management techniques that favour or hinder specific Internet traffic based either on the type, origin or destination of the content (content-based discrimination), or on the type of application or protocol used for data transmission (application-based discrimination).

Works Cited

Anderson, Nate. "Norway's public broadcaster launches BitTorrent tracker." Ars Technica 9 Mar. 2009. Web. 30 Nov. 2009. <http://arstechnica.com/tech-policy/news/2009/03/norways-public-broadcaster-nrk-receives.ars>.

Atkinson, Rob, Ezell, Stephen, Castro, Daniel, and Ou, George. "The Need for Speed: The Importance of Next-Generation Broadband Networks." Information Technology and Innovation Foundation 5 Mar. 2009. Web. 30 Nov. 2009. <http://www.itif.org/index.php?id=231>.

Bell Canada Enterprises. 2007 Annual Report BCE Inc.: Montreal, n.d. Web. 30 November, 2009. <http://www.bce.ca/data/documents/BCE_annual_2007_en.pdf>.

"Best-Effort Service." Encyclopedia of Networking. Ed. Werner Feibel. 3rd ed. San Francisco: The Network Press, 2000. 136. Print.

Bridges, Andy. "Net neutrality: What it is and why does it matter?" College and Research Libraries News. 67.8 (2006). Web. 30 Nov. 2009. <http://www.ala.org/ala/mgrps/divs/acrl/publications/crlnews/2006/sep/washingtonhotline.cfm>.

Campaign for Democratic Media. Initial Comments of Campaign for Democratic Media. Telecom Public Notice CRTC 2008-19: Review of the Internet Traffic Management Practices of Internet Service Providers. CIPPIC, 23 Feb. 2009.

Web. 17 June 2009. <http://www.cippic.ca/uploads/File/Argument_-_CRTC-PN2008-19_-_FINAL_-_23Feb2009.pdf>.

Canadian Heritage. "A Convention on the Protection and Promotion of the Diversity of Cultural Expressions." 4 Nov. 2009. Web. 30 Nov. 2009. <http://pch.gc.ca/pgm/ai-ia/rir-iro/gbll/convention/index-eng.cfm>.

Canadian Library Association (CLA). "Canadian Library Association / Association canadienne des bibliothèques Position Statement on Intellectual Freedom." CLA. 18 Nov. 1985. Web. 30 Nov. 2009. <http://www.cla.ca/Content/NavigationMenu/Resources/PositionStatements/Statement_on_Intell.htm>.

Canadian Radio-television and Telecommunications Commission (CRTC). "2008-04-03 - #: 8622-C51-200805153 - Canadian Association of Internet Providers (CAIP) - Application requesting certain orders directing Bell Canada to cease and desist from throttling its wholesale ADSL Access Services." CRTC. 22 Dec. 2008. Web. 30 Nov. 2009. <http://www.crtc.gc.ca/partvii/eng/2008/8622/c51_200805153.htm>.

--- "Communications Monitoring Report 2008." CRTC, n.d. Web. 24 July 2009. <http://www.crtc.gc.ca/Eng/publications/reports/PolicyMonitoring/2008/cmr2008.htm>.

---. "Telecom Decision CRTC 2008-108. The Canadian Association of Internet Providers' application regarding Bell Canada's traffic shaping of its wholesale

Gateway Access Service." CRTC. 20 Nov. 2008. Web. 30 Nov. 2009. <http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm>.

---. "Telecom Public Notice CRTC 2008-19. Review of the Internet traffic management practices of Internet service providers." CRTC. 20 Nov. 2008. Web. 30 Nov. 2009. <http://www.crtc.gc.ca/ENG/archive/2008/pt2008-19.htm>.

---. "Telecom Regulatory Policy CRTC 2009-657. Review of the Internet traffic management practices of Internet service providers." CRTC 21 Oct. 2009. Web. 30 Nov. 2009. <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm>.

---. "Telecom Decision CRTC 2009-677. Canadian Association of Internet Providers et al. and Vaxination Informatique -- Application to review and vary certain determinations in Telecom Decision 2008-108 related to Bell Canada's Internet traffic management practices." CRTC. 29 Oct. 2009. Web. 30 Nov. 2009. <http://www.crtc.gc.ca/eng/archive/2009/2009-677.htm>.

Canadian Internet Policy and Public Interest Clinic (CIPPIC). "Bell Canada/Bell Sympatico Use of Deep Packet Inspection: PIPEDA Complaint." CIPPIC. 9 May 2008. Web. 30 Nov. 2009. <http://www.cippic.ca/uploads/Bell-DPI-PIPEDAcomplaint_09May08.pdf>.

Cheng, Jacqui. ""Canada's Next Great Prime Minister" to be found on P2P." Ars Technica. 19 Mar. 2008. Web. 30 Nov. 2009.

<http://arstechnica.com/old/content/2008/03/canadas-next-great-prime-minister-to-be-found-on-p2p.ars>.

Chung, Emily. "CRTC to decide on new rules for internet service providers." CBC News. 16 July 2009. Web. 30 Nov. 2009. <http://www.cbc.ca/technology/story/2009/07/15/f-internet-traffic-management-crtc-hearings.html>.

Cisco Systems. White Paper: Controlling Your Network - A Must for Cable Operators. N.p., 1999. Web. 30 Nov. 2009. <http://www.democraticmedia.org/files/Cisco1999WhitePaper.pdf>.

Corbató, Steven C., and Teitelbaum, Ben. Internet2 and Quality of Service: Research, Experience, and Conclusions. N.p., 2006. Web. 30 Nov. 2009. <http://net.educause.edu/ir/library/pdf/CSD4577.pdf>.

De Beer, Jeremy. "The University Shouldn't Shape My Traffic." Jeremy de Beer. 29 Nov. 2007. Web. 30 Nov. 2009. <http://www.jeremydebeer.ca/index.php?option=com_content&task=view&id=191>.

"Declaration of Principles." WSIS. 12 Dec. 2003. Web. 19 May 2010. <http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf>.

Documentary Organization of Canada (DOC). "Telecom Notice of Public Consultation and Hearing CRTC 2008-19. Call for Comments on Internet

traffic management practices of Internet service providers." CRTC. 23 Feb. 2009. Web. 30 Nov. 2009. <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030141.pdf>.

"Download Decade". Globe and Mail. 2009. Web. 30 Nov. 2009. <http://www.theglobeandmail.com/news/technology/download-decade/>.

Federal Communications Commission (FCC). "FCC 02-77 Order". FCC. 14 Mar. 2002. Web. 30 Nov. 2009. <http://www.fcc.gov/Bureaus/Cable/News_Releases/2002/nrcb0201.html>.

---. "New Principles Preserve and Promote the Open and Interconnected Nature of Public Internet". FCC 5 Aug. 2005. Web. 30 Nov. 2009. <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf>.

---. "FCC 09-93 Notice of Proposed Rulemaking". October 22, 2009. Web. December 21, 2009. <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf>.

---. "FCC 08-183 Order". FCC. 20 Aug. 2008. Web. 30 Nov. 2009. <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf>.

Frieden, Rob. "Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers." Fordham Intellectual Property, Media & Entertainment Law

Journal. 18.3 (2008). Web. 30 Nov. 2009. <http://iplj.net/blog/archives/volumexviii/book3>.

Ganley, Paul, and Ben Allgrove. "Net Neutrality: A User's Guide." Computer Law & Security Report 22.6 (2006): 454-63.

Heskett, Ben. "Cisco drawn into Net control battle." CNET News. 30 July 1999. Web. 30 Nov. 2009. <http://news.cnet.com/Cisco-drawn-into-Net-control-battle/2100-1033_3-229285.html>.

IFLA. "IFLA Statement on Libraries and Intellectual Freedom." IFLA. 25 Mar. 1999. Web. 30 Nov. 2009. <http://www.ifla.org/en/publications/ifla-statement-on-libraries-and-intellectual-freedom>.

Industry Canada. "Telecommunications Service in Canada: An Industry Overview. Section 6: The Evolution of Competition in the Canadian Telecommunications Service Market." Industry Canada. 30 July 2009. Web. 30 Nov. 2009. <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf06288.html>.

Information & Instructional Technology Services (IITS). "Checking Your Quota." University of Toronto, Scarborough. 2007. Web. 30 Nov. 2009. <http://webapps.utsc.utoronto.ca/ccweb/services-resnet/checking-your-quota>.

Instructional & Information Technology Services (IITS). Concordia University. Email to the author. 12 May 2009.

Kapica, Jack. "Bell opens a large can of worms." Globe and Mail. 21 May 2008. Web. 30 Nov. 2009. <http://www.theglobeandmail.com/blogs/article685921.ece>.

Longford, Graham. 'Network neutrality' vs. 'network Diversity': A Survey of the Debate, Policy Landscape and Implications for Broadband as an Essential Service for Ontarians. Working paper for the Ministry of Government Services (Ontario). CRACIN, n.d. Web. 27 Jan. 2010. <http://www3.fis.utoronto.ca/iprp/cracin/alttelecomcontent/Longford%20-%20Network%20Neutrality%20vs%20Network%20Diversity.pdf>.

McTaggart, Craig. "Was the Internet Ever Neutral?". Proceedings of the 34th Telecommunications Policy Research Conference. U. of Michigan, School of Information, 30 Sept. 2006. Web. 27 Jan. 2010. <http://web.si.umich.edu/tprc/papers/2006/593/mctaggart-tprc06rev.pdf>.

"Network Neutrality." American Library Association. n.d. Web. 17 May 2009. <http://www.ala.org/ala/issuesadvocacy/telecom/netneutrality/index.cfm>.

O'Connell, Patricia. "At SBC, It's All About "Scale and Scope."" BusinessWeek. 7 Nov. 2005. Web. 30 Nov. 2009. <http://www.businessweek.com/magazine/content/05_45/b3958092.htm>.

Office of the Privacy Commissioner of Canada. "PIPEDA Case Summary #2009-010. Report of Findings. Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection." OPCC. Sept. 2009. Web.

30 Nov. 2009. <http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm>.

---. "Telecom Public Notice CRTC 2008-19 -- Review of the Internet traffic management practices of Internet service providers; CRTC Reference: 8646-C12-200815400." CRTC. 18 Feb. 2009. Web. 30 Nov. 2009. <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1027577.PDF>.

---. "What is Deep Packet Inspection?" Deep Packet Inspection: A Collection of Essays from Industry Experts. OPCC, n.d. Web. 7 Dec. 2009 <http://dpi.priv.gc.ca/index.php/what-is-deep-packet-inspection/>.

Parsons, Christopher. "Deep Packet Inspection in Perspective." New Transparency Project. 10 Jan. 2008. Web. 27 Jan. 2010. <http://www.sscqueens.org/sites/default/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf >.

Press, Larry. "Broadband Policy: Beyond Privatization, Competition and Independent Regulation." First Monday 14.4 (2009) Web. 27 Jan. 2010. <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2374/2159>.

Riley, M. Chris, and Ben Scott. Deep Packet Inspection: The End of the Internet as we Know it. Free Press, 2009. Web. 22 July 2009.

<http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf>.

Sandvig, Christian. "Network Neutrality is the New Common Carriage." Info : the Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media 9.2/3 (2007): 136.

Shaw, Russell. “Cable broadband ISP's QoS enhancement surcharge draws Vonage's ire.” ZDNet. 7 Mar. 2006. Web. 16 Jun. 2010. <http://www.zdnet.com/blog/ip-telephony/cable-broadband-isps-qos-enhancement-surcharge-draws-vonages-ire/952>.

Telecommunications Act, R.S.C. 1993, c. 38. Department of Justice Canada. 23 Nov. 2009. Web. 30 Nov. 2009. <http://laws.justice.gc.ca/en/T-3.4/FullText.html>.

Telus Blocks Consumer Access to Labour Union Web Site and Filters an Additional 766 Unrelated Sites. OpenNet Initiative, 2 Aug. 2005.Web. 22 July 2009. <http://opennet.net/bulletins/010/>.

Topolski, Robert M. NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking. Free Press. 2008. Web. 30 Nov. 2009 <http://www.freepress.net/files/NebuAd_Report.pdf>.

UNESCO. "Convention on the protection and promotion of the diversity of cultural expressions 2005." UNESCO. 20 Oct. 2005. Web. 30 Nov. 2009

<http://portal.unesco.org/en/ev.php-URL_ID=31038&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

Wilson, K. G. "The Last Mile: Service Tiers Versus Infrastructure Development and the Debate on Internet Neutrality." Canadian Journal of Communication 33.1 (2008): 81-100. Print.

Wu, Tim, and Christopher S. Yoo. "Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate." Federal Communications Law Journal 59.3 (2007): 575-592. Print.

Wu, Tim. Network Neutrality FAQ. N.p., n.d. Web. 22 July, 2009. <http://www.timwu.org/network_neutrality.html>.