Interpreting Network Discrimination in the CRTC and FCC

Mark Perry
Dept. of Computer Science - Faculty of Law
University of Western Ontario
London, Ontario
mperry@uwo.ca

Thomas Margoni
Dept. of Computer Science - Faculty of Law
University of Western Ontario
London, Ontario
tmargoni@uwo.ca

***Abstract*—The issue of what discriminatory use of a network means has arisen in two recent decisions of the United States and Canadian federal communications commissions, the FCC and the CRTC respectively. The topic is a contemporary and hotly debated one, as when a course is fixed it will strongly influence the future of the Internet. It can be stated as the dichotomy of open and competitive or closed and oligopolistic. A study and comparison of the two different approaches is vital to clarify the debate, and hopefully guide Canadian policy in a direction that will benefit the whole community.**

***Keywords*-Traffic Shaping, Deep Packet Inspection, Network Neutrality, Packet Discrimination, Policy**

I. Introduction

The issue of Network Neutrality first loomed large on the Canadian landscape just some years ago, with a case of (network) discrimination, or rather discriminatory network use. Telus, a Canadian telecommunications company, blocked the access to a website supporting the union with which it was in dispute in 2005. The website, was allegedly "run by and for Telecommunication Workers Union" members.[1] Despite questions of freedom of expression and the right to lawfully strike raised in this case, in this paper we are focusing on discrimination of a different kind, namely against individual packets on the internet. Blocking, as in the Telus case is an example of blunt discriminatory use of network control. Advances in computing technologies allow for more sophisticated control of communications. For example, although Deep Packet Inspection (DPI) is a technique known for over ten years, such tools were not feasible for large scale use until these last few years back. DPI, differently from Static and Stateful Packet Inspection, enables the monitoring of packet content in addition to packet headers.

The following sections will give an overview of how ISPs usually manage their networks, make a comparative legal analysis of the U.S. and Canadian federal communications commission decisions with an explanation of how packets are treated on switched packet networks, provide some data of a limited series of experiments we have conducted and compare the results with the relevant contractual agreements, and conclude with a strong recommendation for the future of a wealthy Canadian open and competitive Internet. Although there has been activity in other countries [2][3], we focus here on North America.

II. Network management

Two recent examples illustrate DPI use. The Canadian Association of Internet Providers (CAIP) alleged traffic shaping and throttling by Bell Canada in a complaint to the Canadian Radio Television and Telecommunication Commission (CRTC). Bell Canada has publicly declared that it uses network shaping by limiting Point to Point (P2P) through DPI.[4] The CRTC rejected all claims and held this Bell Canada activity legitimate. In a similar case, the U.S. Federal Communications Commission (FCC) analysed the behaviour of Comcast in response to numerous complaints received about its quality of service. It involved P2P, in particular BitTorrent. The FCC ordered Comcast to "end discriminatory network management practices". Comcast has appealed, alleging that the Federal Communications Commission lacks any authority to enforce rules on federal communications.

We believe, as did the FCC, that ISPs violate legislation surrounding telecommunications and privacy. DPI enables ISPs to monitor and collect packet content. We do not examine the technology in detail as there are many papers on DPI and its application. [5] The kind of information that can be gathered through these tools, beside potentially violating users' privacy, enables ISPs to engage in activities that belie consumer protection, competitive market regulation and other non-discriminatory economic rules and fundamental rights. In some countries DPI has been used for censorship purposes, and not only passively (blocking "dangerous" connections), but allegedly also actively, meaning that it is possible to modify the content of the communication without either sender and receiver's knowledge. For example, the ISP could delete words that it does not like, and substituting with others more 'acceptable'[6].

A. *Effects of network management*

Why do ISPs engage in activities unpopular with their customers, particularly when such efforts are expensive to operate? There are several answers. In general the usual

arguments made at this regard may be summarised as follows:

1) A usable and healthy Network: To avoid a too high usage of the bandwidth by a few categories of users and to fix problems of slow and congested networks, bottlenecks, and similar problems (allegedly caused not by low investment in infrastructures, but by high usages of P2P networks). Many counter argue that the easy way to get this is to allocate a limited amount of bandwidth to any user and limit its usage to this given amount. The sum of the total amounts is what a given piece of network is able to carry. However, what usually happens in the wholesale (and also retail) market of cable companies and ISPs is quite similar to the behaviour known as 'overbooking' by air companies: since statistically speaking is very unlikely that all the users use all their allocated bandwidth at the same time, it is possible to sell more bandwidth than that available, in a way that increases revenues with a very little probability of vexing users. Sometimes this same argument is sold as a benefit to users, auguing that they get more for their money.

2) Price discrimination: By dividing the market, ISPs can internalise the maximum consumer surplus. If an ISP can determine that some categories of users are interested only in basic services, say surfing and emails, while others need more variegate services, like connecting to VPN servers and VoIP, and the ISP is further able to accordingly shape/limit connections, then it will be able to sell the basic service to those customers who wouldn't pay a higher fee for extra services, while still charge a higher price to those who need the extra services. In this way, *i.e.*, through market segmentation, ISPs are able to charge the maximum price that each category is willing to pay for a given service and internalise a great share of consumer surplus, raising revenue but disadvantaging consumers. Such a situation is typical of those markets characterised by non perfect competition, *e.g.* oligopolies.

3) Vertical integration economies: The same company may own the cable, sell the connectivity, and offer related services (*e.g.* content purchase, emails, hosting, Television, VoiP, etc). The problem here is that of unfair competition, *i.e.*, if the company is a telephone company it is probably not happy with consumers using VoIP solutions, or at least not third party VoIP services that are sometimes a free of charge. If the ISP is a TV company, then you should rent its films, and not from another online store, or at least if one does it through her ISP store the download speed is faster. This kind of vertical integration represents a typical anticompetitive behaviour.

III. An analysis of the two decisions

In its Telecom Decision CRTC 2008, 108 of November 20th, 2008 the CRTC declared that if a huge cable company applies the same kind of network shaping and throttling to both wholesale and retail customers there is no discrimination. From one perspective this is correct, as there is no discrimination between wholesale and retail customers in terms of the reduction of network freedom to which they are entitled. Network freedom here means the possibility to do with the network anything that you want (excluding those acts that constitute criminal behaviour). The CRTC ignored the impact that the more technical, often unperceived, but increasingly important kind of discrimination, that towards packets. The network owner, or at least a physical piece of it, can decide which packet should arrive first, which should arrive last, and which should not arrive at all. Since packets represent everything transmitted over the internet, from the recipe for apple pie to a video stream, from VoIP to unknown (because encrypted) data flows, the importance and trickiness of the issue is clear. The default for the internet (TCP/IP) is based on sending pieces of data over the net as fast as possible. Communications are chunked into packets that are sent over the network toward their common destination. Packets of the same communication may take different routes to get to destination in the most fast, efficient and non-congested way. So, packets of different kind and of different communications travel together around the network. The way in which they are delivered, the general rule, is first-in first-out This kind of design implies that there is not packet discrimination connected with the source, destination, content, type, carrier, etc. Every packet is treated equally. For example every packet suffers the same way and amount of latency, even regardless whether the packet is of a kind that is time-sensible or not (audio-video packets are treated like http packets, even though they are differently affected by delays in delivery). For this very reason it is argued that the internet, beside the fact that TCP/IP is open and publicly available, and it follows an end-to-end design, has grown so fast.[7]

A. What the CRTC believes to be discriminatory

The CRTC took into consideration in its decision the discrimination between wholesale and retail customers. It missed the point. Nonetheless, the decision has some interesting passage, especially in terms of network shaping and privacy concerns. Bell Canada declares that it is engaged in traffic shaping on its network, which consist of slowing down the transfer rates of all P2P file-sharing applications during peak periods, using DPI on a network-wide bases.[8] Bell Canada engages in this as the best practical approach to address network congestion together with capacity investments and implementation of usage-based pricing.[8] Bell Canada alleges that customers are aware of this activity since in its Terms of Service (art. 8.3 item 10), and that "Customers are prohibited from using Bell Canada's services or permitting them to be used so as to prevent a fair and proportionate use by others. For this purpose, Bell Canada may limit use of its services as

necessary".[8] CAIP, which was the applicant to the CRTC for a cease and desist order to Bell to stop traffic shaping. There were many interveners and comments (over 1,300) some of whom noted discrimination caused by the undue disadvantage towards those users and services that rely on P2P architecture, which is a wide category, embracing for example Skype phone and video calls, other applications suffered slowdown effects caused by the throttling activities. In particular Virtual Private Network (VPN) and other encrypted traffic (such as many VoIP services). Applicants also sustained that Bell Canada was granting itself a preference in the retail market by degrading the bandwidth services that it provides to ISPs. CAIP explicitly submitted that the bandwidth being freed up by Bell Canada was being re-allocated to the company's other services, such as its upgraded 'Max' DSL services, its online video store, and Internet Protocol Television (IPTV), service. CAIP alleged violations of the Canadian Telecommunication Act, sections 24 (Conditions of Service approved by Commission), 25(1) (Violation of Commission approved tariffs), 27(2) (Unjust discrimination of service or charging) and 36 (Prohibition of control or influence of communications), and of the general principle of contributing to the protection of the privacy of persons (art. 7(i)). It is not the objective of this paper to analyse in great detail the CRTC decision: it is enough to note that the CRTC rejected all the allegations of CAIP *et al*. and accepted all the counter claims of Bell Canada.

B. FCC and the open Internet

The U.S. Federal Communications Commission in the Memorandum Opinion and Order FCC 08-183 EB-08-IH-1518 (FCC Order), discussing the formal complaint of Free Press *et al*. against Comcast shows a totally different attitude. Comcast was not only degrading P2P connections, but was engaged in a quite more intrusive activity: sending packets to applications with the Reset flag, meaning that was closing, not only slowing down, connections between users "like a telephone operator that interrupts a phone conversation, impersonating the voice of each party to tell the other that 'this call is over, I'm hanging up' ".[9] Apart from the latter, many of the other circumstances are similar to those giving rise to the Bell Canada CRTC decision. The FCC approach was different from the start: "although Comcast asserts that its conduct is necessary to ease network congestion, we conclude that the company's discriminatory and arbitrary practice unduly squelches the dynamic benefits of an open and accessible Internet and does not constitute reasonable network management" (p.1 FCC Order). The FCC immediately recognises the issue of vertical integration of carriers and their interest in sending content, and thus to privilege on their wires their own content, thereby limiting users' freedom of choice: "P2P applications [...] have become a competitive threat to cable operators such as Comcast because Internet users have the opportunity to view high-quality video with BitTorrent that they might otherwise watch (and pay for) on cable television. Such distribution poses a particular competitive threat to Comcast's video-on-demand (VOD) service" (p.3 FCC Order). The FCC established that Comcast discriminated among applications and protocols rather than treating all equally. This was done by deploying equipment across the network to monitors TCP connections using DPI. The FCC: "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". The FCC also observes more generally that such kind of network shaping has also a high potential of anticompetitive abuse, as far as such practice selectively blocks and impedes the use of particular applications, thereby disadvantaging these application into the market. Further, such anticompetitive attitude perpetuated by discriminatory network management practices is clearly compounded by failing to disclose such practices to consumers (p.31 FCC Order). The FCC does not disregard the legitimate interest of ISPs to manage their bandwidth, and recognises that since "consumers are entitled to access the lawful Internet content of their choice" the providers, in a way which is consistent with federal policy, may block transmissions of illegal content or transmissions that violate copyright law. However, the conclusion in this case does not leave any doubt regarding the nature of such network management. To the extent that providers choose to utilise practices that are not applications or content neutral, the risk to the open nature of the Internet is particularly acute and the danger of network management practices being used to further anticompetitive ends is strong (p.31 FCC Order).

C. Two countries separated by a common language

The FCC decision has impressed many commentators for the clearness of the statements and the strong support of an open and competitive Internet. The reason is not simply a developed sensibility towards telecommunications or for renown support for a highly competitive rather than oligopolistic market. The relevant legislation is key. The U.S. Telecommunication Act of 1996 gives good policy guidance with regard of the direction that the Internet should follow. It states that it is a federal policy to promote the development of the Internet, to preserve its vibrant and competitive free market, and to encourage the development of technologies that maximise user control over what information is received. [10] On its side, the FCC, empowered at this regard by the Telecommunication Act, developed in 2005 the Internet Policy Statement[11] where it sets forth four principles with the intent to "encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet" and enable consumers: to access the lawful Internet Content of their choice; to use services of their choice; to connect the devices of their choice that do not harm the network; and to enjoy of a competitive

market among network, application, content and internet providers.[11] More recently, the new FCC commissioner has officially expressed his intention to create two new principles that are particularly relevant. The first would prevent Internet access providers from discriminating against particular Internet content or applications, while allowing for reasonable network management, whereas the second principle would ensure that Internet access providers are transparent about the network management practices they implement.[12]

In the Canadian Telecommunication Act of 1993 the word Internet is not contemplated. Given this legal and socio-economic environment, it should not surprise why the U.S. telecommunication market is much more developed than its northern neighbour. So, within this legal framework, it is no surprise that the CRTC has taken a prudent approach by refusing to enter into a such thorny problem. It would have implied a strong policy taking with a not very strong but still arguable jurisdiction. The CRTC has preferred to make a public call for comments regarding the "Internet traffic management practices of Internet service providers".[13] It will be of paramount importance.

IV. Data

During the month of September 2009 we ran some tests on three major Canadian ISPs: Rogers, Primus and Bell Canada.[16]. The aim was to see whether the Internet connection users have at their disposal suffers of any form of shaping, throttling or discrimination. The tools used to test networks are publicly available and in many cases are FLOSS tools.[15] We mainly used one tool: Glasnost.[14] With regard to Rogers, Glasnost says that the network throttles BitTorrent Traffic (BTT) on a port non-standard for BTT (10009) in upload, and also that all TCP traffic on port 6881 (standard BTT port) is throttled, in upload. Rogers intervened on the side of Bell Canada in the CRTC decision (at sec. 23) in order to sustain and give more weight to Bell's positions on the necessity of network shaping. This reduced the speed of the traffic to around 10% of unthrottled traffic.

The same test with Primus shows that Primus is not engaged in any network shaping activity regarding BTT. This again is somehow not surprising since Primus took the side of the CAIP in the CRTC decision (sec. 24).

Finally we tested Bell Canada, and here the result is some how unexpected since it appears that at least during our tests and on the connection we have tried there is no network shaping on BTT. We said this is quite surprising since what Bell Canada declared at the CRTC, *i.e.*, that they are engage in such activities.

A. Are users aware of network shaping?

We have checked the contracts that these three Canadian ISPs make with users when they get connected. We have relied on the documentation that the companies make available on their websites. In no document is there present a clear statement regarding network shaping or DPI.

Rogers in its Rogers Services Terms and Conditions does not refer explicitly to any kind of network shaping, throttling or DPI. In this document we may identify some general statement, which is so vague that it could be argued its function could be that of informing users of some form of monitoring. For example sec. 17 reads:"We reserve the right to restrict, change, suspend or terminate your Service by any means if your access, use or connection to the Services, Equipment or our facilities is impairing or adversely affecting our operation or the use of our Services or facilities by others". In sec. 19 the word 'monitoring' is used: "We have the right, but not the obligation, to monitor or investigate any content that is transmitted using the Services or the Equipment. We may also access or preserve content or information to [...] operate the Services, ensure compliance with the Service Agreement or any Policies, or protect ourselves, our customers or the public". Some more specific wording may be found in a separate document, present on the same webpage reported above. In the 'Acceptable Use Policy' at page 5 it is observable the label 'Network Management' that reads: "We reserve the right to manage our network in order to optimize its efficiency for the benefit of our subscribers, including, without limitation, by way of the following: rate limiting (speed), [...] and protocol filtering. We may take any other action we deem appropriate in order to help ensure the integrity of the network experience for all subscribers". This wording that could represent a more clear confirmation of what kind of monitoring activities the ISP is engaged in, do not appear to apply to the Terms of Services of Rogers Yahoo! High-Speed Internet, which is our case. In fact, in the latter, sec. 34 apparently excludes any external contractual integration source:'34. The Service Agreement, as amended from time to time, constitutes the entire agreement between you and Rogers for the Services and supersedes all prior agreements, written or oral, with respect to the same subject matter".

In the case of Primus, which from our limited tests is not engaged in any network shaping, in the Acceptable Use Policy, at sec. 5 we have: "System Resource and Utilization: a) Primus will use all commercially reasonable efforts to allocate system resources. As part of resource allocation, Primus may limit, restrict or prioritize access to system resources, including CPU time, memory, disk space, session length, and number of sessions. b) Primus reserves the right to institute services and fees for account holders who are interested in accessing system resources above and beyond acceptable usage [...]".

Finally in case of Bell, which declared in the past to be engaged in network throttling and DPI but that resulted not doing this during our test, the relevant contractual documentation at sec. 17 reads: "However, you agree that

Your Service Provider reserves the right from time to time to monitor the Service electronically, monitor or investigate content or your use of Your Service Providers networks, including without limitation bandwidth consumption, and to disclose any information necessary [...] to operate the Service or to protect itself or others". Further, in the 'Acceptable Use Policy', sec. 'General', one may read: [it is prohibited to] Restrict[ing] or inhibit[ing] any other user from using or enjoying the Internet, impairing the operations or efficiency of the Service or creating an unusually large burden on our networks, or otherwise generating levels of Internet traffic sufficient to impede other users ability to transmit or receive information". Bell Canada, further, reserves itself the "sole right to review materials sent through such service [Bell Canada Email Service], and to remove any materials in their sole discretion". Apparently Bell Canada has updated their Terms of Service since the CRTC decision.

It is interesting, especially from the consumer (and citizen) point of view, to compare test results with the contractual agreements here analysed. In fact, a first blush conclusion is that borrowing the FCC wording "the anticompetitive harm perpetuated by discriminatory network management practices is clearly compounded by failing to disclose such practices to consumers. Many consumers experiencing difficulty using only certain applications will not place blame on the broadband Internet access service provider, where it belongs, but rather on the applications themselves, thus further disadvantaging those applications in the marketplace".[9]

V. Conclusions

From what we have seen above, the future of Network Neutrality in Canada is going to be delineated 'here and now'. The first skirmish is over, but the next confrontation is undoubtedly close. The CRTC is going to play an important role on the evaluation of what Internet means for Canada. In this sense, the balance struck by the FCC may represent a good starting point. Nobody denies the interest of ISPs in managing their networks in order to offer a better service to users, but at the same time there are activities that do not fit into the concept of network management. To arbitrarily decide which kind of packets and communication deserves priority, which may be slowed down, and which dropped, is a form of discrimination that is not consistent with the nature of Internet.

To spy on users is another good example. Either there is no spying, or there are illegitimate intrusions in people's lives and communications. We do not believe that such intrusions are the same as those reported in non-democratic countries, but the tools are the same. Information and telecommunication infrastructures deserve the same level of consideration that their 'off-line' parallels have, for they represent the future evolution of how individuals living in a given country enjoy an e-democratic, participative and accountable society. From an economic and business perspective, there are market behaviors based on vibrant competition, that allowed the Internet to become what it is: Google, Facebook, Skype, Yahoo!, and many more would have never had the chance to spread in a non-neutral environment. There are other market behaviors based on monopolistic and oligopolistic models that not only reduce users' surplus, but also the general societal welfare for everybody. This latter has not represented the Canadian tradition up to now.

A last reasons why Network discrimination should be avoided, especially if based on intrusive tools like DPI is one that the very same ISPs must not have considered adequately. In a system where such debate is much more developed than Canada (the U.S. again) many arguments have been made in the sense that the usage of DPI would disqualify ISPs from liability exemptions.[17] Briefly, the Digital Millennium Copyright Act (DMCA) with regard to secondary and vicarious copyright infringement has created some exemptions (safe harbours) for ISPs in specific situations, that here we could generally describe as where ISPs operate as mere conduits. If ISPs do not know what is being transmitted through their networks, and their activity is limited to carry such bits, there is no liability on ISPs shoulders. Things obviously change if ISPs know what is transmitted over their wire. Since DPI especially in the way is currently implemented allows for a general, network wide, knowledge of what content is transmitted in real time, is quite likely that this disqualify ISPs from DMCA safe harbour provisions. This is much likely something that ISPs do not want, since it would mean that they may be held liable for almost any copyright infringement occurred on their wires and cables.

On the Canadian landscape, such a debate has yet to gain much centrality. Canada has no legislation, at the moment, that may be compared to the DMCA. However, from the Copyright Act and some relevant case law[18][19], it is arguable that as far as ISPs behave as mere conduits, do not perform any act related to content, and do not have any control on the content exchanged, they may benefit from the 'Intermediary exception' provided by sec.2.4(1)(b) Canadian Copyright Act. In the absence of any specific legal provision at this regard, it is arguable that if ISPs behave as mere conduits they are reasonably safe regarding copyright liability. If they engage in network management in a way that allows them to know what content is transmitted and to have control over it, by means of giving it priority, slowing it down, or resetting it completely, than ISPs may have opened the door for being considered liable for copyright infringement (not to mention other liabilities such as defamation, and furthermore invasion of privacy and potentially illegal interception if their contracts are not clear). The question is: who benefits from a non-neutral network?

ACKNOWLEDGMENT

The authors thank the Social Science and Humanities Research Council, the Natural Science and Engineering Research Council for their support.

REFERENCES

[1] http://www.cbc.ca/canada/story/2005/07/24/telus-sites050724.html. All the websites cited in this work have been last visited during October 2009.

[2] S. Fernandes - R. Antonello - T. Lacerda - A. Santos - D. Sadok - T. Westholm, *Slimming Down Deep Packet Inspection Systems*, SITE, Univ. of Ottawa, Ottawa, ON; This paper appears in: INFOCOM Workshops 2009, IEEE Publication Date: 19-25 April 2009 On page(s): 1 - 6

[3] A. Glorioso - V. Vitkov, *Accesso ad Internet e contratti di connettivit business to consumer di quattordici fornitori italiani*, in Diritto dell'informazione e dell'informatica, 2009, available at: http://nexa.polito.it/sites/nexa.polito.it/files/contratti-nn-final-2008-11-24.pdf

[4] See "General Position of the Parties n.7", available at http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm.

[5] G. Goth, *ISP Traffic Management: Will Innovation or Regulation Ensure Fairness?*; This paper appears in: Distributed Systems Online, IEEE, Publication Date: Sept. 2008 Volume: 9 , Issue: 9 On page(s): 2 - 2

[6] B. Wagner, *Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'*, Global Voices Advocacy, 2009.

[7] M. A. Lemley - L. Lessig, *End to End: The Architectural Principle of Open Access*, Ex Parte Declaration In re: MediaOne Group, Inc. to AT&T Corp., FCC. CS Docket No. 99-251 (Dec. 1999).

[8] Canadian Radio-television Telecommunications Commission, *Telecom Decision CRTC 2008-108*, sec. 6 and 7.

[9] Federal Communication Commission, *Memorandum Opinion and Order FCC 08-183 EB-08-IH-1518*, pp.24, footnote 181.

[10] See 47 U.S.C. Sec. 230(b)(1)(2) and (3).

[11] Federal Communications Commission, *Internet Policy Statement*, FCC 05-151.

[12] FCC Official Communication of September 21, 2009.

[13] CRTC Telecom Public Notice CRTC 2008, of November 19, 2008.

[14] See http://broadband.mpi-sws.org/transparency.

[15] See http://www.measurementlab.net.

[16] See www.rogers.com; www.primus.ca; and www.bell.ca.

[17] R. Frieden, *Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers* (June 2007). Available at SSRN: http://ssrn.com/abstract=995273.

[18] See *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers* [2004] 2 S.C.R. 427, 2004 SCC 45, 240 D.L.R. (4th) 193, 32 C.P.R. (4th) 1.

[19] See *CCH Canadian Ltd. v. Law Society of Upper Canada* [2004] 1 S.C.R. 339, 2004 SCC 13, 236 D.L.R. (4th) 395, 30 C.P.R. (4th) 1, 247 F.T.R. 318.