

TELECOMMUNICATIONS POLICY REVIEW SUBMISSION

Professor Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa, Faculty of Law

August 2005

INTRODUCTION

I am a law professor at the University of Ottawa where I hold the Canada Research Chair in Internet and E-commerce Law. I also write a weekly law and technology column that appears in the Toronto Star, Ottawa Citizen, and Canada.com. My comments, which are drawn from earlier published work in the area, focus on the relevancy of the *Telecommunications Act's* objectives (**Issue B1**) to the current Internet environment. I discuss three key policy objectives – universal broadband access (**Issue D6**), legislated network neutrality (**Issues B32, F1**), and Internet privacy protection (**Issue B31**). I argue that section 7 of the *Telecommunications Act* can be interpreted to cover each objective but that additional legal and policy provisions are needed to effectively implement such objectives.

INTERNET TELECOMMUNICATIONS POLICY PRINCIPLES

Given my interest in effectiveness of the current *Telecommunications Act* for the purposes of Internet telecommunications, I believe that the panel would do well to focus on three questions: (i) what key principles should form the core of Internet telecommunications policy? (ii) are those principles found in the current Act? and (iii) if so, are the principles effectively being implemented into law?

I believe that the answer to the first question rests with three principles: universal broadband access, network neutrality, and Internet privacy.

I. UNIVERSAL BROADBAND ACCESS (Issues D2, D3, D5, D6, D9)

While high-speed Internet access (often referred to as broadband) is available in most urban areas in Canada, the majority of communities, particularly those on the outskirts of major cities as well as in rural areas, are still without broadband access. In an age when Internet connectivity is increasingly a pre-requisite for banking, health care information, government services, and personal communications, ensuring that an entire community enjoys affordable access is a necessity, not a luxury.

Due largely to the widespread implementation of cable, the populations of most major Canadian cities enjoy access to broadband. In fact, according to a 2003 Statistics Canada study, 86 percent of Canadians have accessibility to broadband services (though a smaller number are actual subscribers).¹ While those figures are impressive, they tell only part of the story. Statistics Canada also reported that just 28 percent of Canadian communities

¹ B. Veenhof, P. Neogi and B. van Tol “High-speed on the Information Highway: Broadband in Canada” (Sept. 2003) Statistics Canada, <<http://www.statcan.ca/english/research/56F0004MIE/56F0004MIE2003010.pdf>> at p. 18.

have access to broadband, suggesting that there is a significant digital divide between urban and rural communities in Canada.

The federal government sought to bridge this divide in 2001 when it launched its much-publicized broadband task force, which was asked to develop a strategy to ensure broadband availability to every Canadian community by 2004. It concluded that underserved communities need a link to the national network together with plans to connect public institutions, local businesses, and residents. The task force acknowledged that market forces alone were unlikely to solve the issue.²

Sadly, Ottawa responded to the task force report by only launching several pilot projects, including Broadband for Rural and Northern Development, which brought broadband connectivity to 1300 communities, as well as the National Satellite Initiative, which sought to develop satellite linkages to far north communities.

Several Canadian municipalities have already come to recognize the need for broadband leadership. The city of Calgary has installed wireless access in several downtown locations, while Kamloops, British Columbia has focused on wireless access in public buildings.

The undisputed Canadian municipal leader is Fredericton, New Brunswick, which identified the need to develop community wireless connectivity in 1999. That led to the Fred E-Zone, which today virtually blankets the entire downtown core with free wireless connectivity. The city has future plans to expand coverage to the full business core along with all public spaces.

While many Canadian communities may follow Fredericton's lead, it falls to the government to bridge this Canadian digital divide. My prior articles on this specific issue have generated significant reader response with the overwhelming majority of respondents pointing to the economic and cultural disadvantage borne by citizens living in communities that do not have broadband access.³ It should be noted that many respondents live in bedroom communities to major cities such as Toronto and Ottawa.

Many expressed frustration that the competitive broadband environment favours those communities with established cable networks. For those outside such communities, there appears to be little incentive for either the phone or cable companies to invest in broadband services. The result is a broadband marketplace that features a telco-cable

² Canada, National Broadband Taskforce, *The New National Dream: Networking the Nation for Broadband Access Report of the National Broadband Task Force* (Ottawa: Industry Canada, 2003) <<http://broadband.gc.ca/pub/program/NBTF/broadband.pdf>>.

³ Michael Geist "Let Towns, Cities Provide Cheap, Everywhere Broadband" *The Toronto Star* (Feb. 2005), <http://www.michaelgeist.ca/resc/html_bkup/feb282005.html>

duopoly for those with broadband access and no broadband whatsoever for communities without cable competition.

In my view, the solution to this significant problem is clear -- **where cable and telephone providers have proven unable or unwilling to offer commercial broadband services, federal, provincial and local governments should fill the void** to ensure that all Canadians enjoy access to e-commerce, distance education opportunities, tele-health, and e-government services. In fact, **even in communities with both cable and telco broadband choices, local municipalities should consider offering a third, publicly supported broadband alternative using a utility model.** The timeframe for such an initiative must also be a priority with the goal of universal broadband access to all Canadians by the end of 2008.

II. NETWORK NEUTRALITY (Issues B32, F1)

Although not directly addressed in the consultation document, I believe that one of the most critically important legislative reforms is the establishment of a principle of network neutrality that would prohibit Internet service providers from blocking content or placing competing services at a disadvantage. ISPs always seem to get the first call when a problem arises on the Internet. Lawmakers want them to assist with investigations into cybercrime, parents want them to filter out harmful content, consumers want them to stop spam, and copyright holders want them to curtail infringement. Despite the urge to hold ISPs accountable for such activities, the ISP community has been remarkably successful in maintaining a position of neutrality, the digital successor (in spirit and often in fact) to the common carrier phone company.

Adopting a neutral approach has always required strict adherence to one cardinal rule: **that ISPs transport bits of data without discrimination, preference, or regard for content.** That rule has served ISPs very well in Canada. When the federal government amended the *Canadian Human Rights Act* to remove lingering uncertainty about its application to hate on the Internet, ISPs were exempted from liability.⁴ Similarly, when Ottawa established rules to address the removal of online child pornography, it consciously avoided placing ISPs in the role of judge and jury by requiring them to take down offending content only after receipt of a court order.⁵

Most recently, Bill C-60, Canada's proposed copyright reform, envisions the creation of a "notice and notice" system for allegedly infringing copyright material online.⁶ That

⁴ *Human Rights Act*, R.S. 1985, c. H-6, s. 13 (3), <<http://laws.justice.gc.ca/en/H-6/31435.html#section-13>>

⁵ *Criminal Code*, R.S. 1985, c. C-46 s. 164.1, <<http://laws.justice.gc.ca/en/C-46/42339.html#section-164.1>>

⁶ Bill C-60 *An Act To Amend The Copy Right Act*, s. 18 <http://www.parl.gc.ca/PDF/38/1/parlbus/chambus/house/bills/government/C-60_1.PDF>

system mirrors the child pornography approach by leaving it to the courts to determine when content should be taken offline.

In fact, Canadian courts have also respected the ISPs' role as intermediaries, setting a high threshold for revealing subscriber personal information in the file sharing lawsuits and upholding their neutrality in last summer's *Tariff 22* decision, a Supreme Court of Canada case involving online music streaming.⁷

Given the importance of the neutrality principle, it is surprising to learn that Canadian law does not appear to currently provide a definitive legal requirement to maintain such neutrality. This became evident in late July 2005 when Telus, Canada's second largest telecommunications company, actively blocked access to *Voices for Change*, a website supporting the Telecommunications Workers Union. Telus was embroiled in a contentious labour dispute with the union, yet its decision to unilaterally block subscriber access to the site was unprecedented.

The company argued that content on the site raised privacy and security issues for certain of its employees. Nevertheless, the blockage of the site was completely ineffective since it remained available to anyone outside the Telus network. Moreover, those within the Telus network could access the site with a bit of creative Internet surfing.

The appropriate approach for Telus would have been the same formula it advises law enforcement and copyright holders to follow -- to obtain a court order to get the site removed. In fact, that was precisely what Telus ultimately did. By first unilaterally blocking the site, however, Telus raised a host of challenging legal issues. The company argued that its subscriber contract granted it the right to block content. While that may be true for its roughly one million retail subscribers, the blockage occurred at the Internet backbone level, thereby blocking access for other ISPs (and their customers) that use Telus as their provider.

For example, Prince Rupert, a small city on the northwest coast of British Columbia, has established a community ISP to provide its citizens with municipally supported Internet access. Since their connectivity is provided by Telus, the entire community found itself unable to access the *Voices for Change* website.

Moreover, the OpenNet Initiative, a joint University of Toronto and Harvard University project, investigated the unintended consequences of the networking blocking and found that by singling out the *Voices for Change* website, Telus blocked an additional 766

⁷ *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, <<http://www.canlii.org/ca/cas/scc/2004/2004scc45.html>>, [2004] 2 S.C.R. 427 [SOCAN cited to S.C.R.].

websites that shared the same IP address.⁸ These included a breast cancer fundraising site, a Colorado-based electronic recycling company's site, and an Australian alternative medicine site.

Canadian law also raises some interesting questions. While not directly applicable to a private sector company, the Charter of Rights and Freedoms guarantees Canadians "freedom of thought, belief, opinion and expression."⁹ The Supreme Court of Canada has ruled that those rights extend to both the speaker as well as the listener.¹⁰ Telus may not have been subject to the Charter, but surely all Canadian corporations should aspire to abide by its principles.

The *Telecommunications Act* may also be relevant to this situation, though the CRTC's 1999 New Media decision to take a hand-off approach to the Internet may diminish its applicability.¹¹ Section 27(2) forbids unjust discrimination in the provision of a telecommunication service. This section is primarily applicable to competing services, though the blocked website may well fit within the definition. Moreover, Section 36 of the Act provides that a "Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public."¹² The CRTC has sought to limit the applicability of this provision to retail end-user Internet services, yet it is clear that the Telus action extended well beyond its own retail customers.

In an era where limited broadband competition and growing convergence leaves providers with economic incentives to favour their own (or affiliated content) over competing services or offerings, **content neutrality in the provision of network services is an absolutely essential principle that should be firmly established under Canadian law backed by regulatory oversight and significant penalties for compliance failures.** The power of the Internet to foster public participation, provide greater cultural choices, and exposure to educational opportunities rests on a principle of unrestricted access to such content. The Telus incident demonstrated that Canadian law does not provide sufficient support for such a principle.

The issue of network neutrality is not limited to content. It is also a core principle in the availability of applications running on the network. A current example in this regard involves VoIP services. Third party providers fear that the established telephone and cable companies will use their advantageous positions to favour their own services to the

⁸ "Telus Blocking of Labor Union Web Site Filters 766 Unrelated Sites" (Aug. 2005) Open Initiative Bulletin 010, <<http://www.opennetinitiative.net/bulletins/010/ONI-010-telus.pdf>>.

⁹ *Constitution Act 1982*, s. 2(b), <http://www.canlii.org/ca/const_en/const1982.html#freedoms>.

¹⁰ *Ford v. Quebec (Attorney General)*, 1988 SCC 94 <<http://www.canlii.org/ca/cas/scc/1988/1988scc94.html>>, [1988] 2 S.C.R. 712 [*Ford* cited to S.C.R.].

¹¹ Canada, CRTC *Public Notice: New Media*, (Ottawa: May, 1999), <<http://www.crtc.gc.ca/archive/ENG/Notices/1999/PB99-84.HTM>>.

¹² *Telecommunications Act*, 1993, c. 38 s. 27 (2), <<http://www.canlii.org/ca/sta/t-3.4/sec27.html>>

detriment of competing, low cost services. In its May 2005 VoIP decision, the CRTC declined to establish a prohibition on high-speed Internet access providers that engage in packet preferencing by either blocking or impairing competing VoIP service.¹³ The CRTC concluded that there was no evidence that packet preferencing represents a real risk.

In recent months, it has become apparent that the opposite is true. The Federal Communications Commission, the CRTC's U.S. equivalent, has ordered at least one ISP to cease blocking a third party VoIP service.¹⁴ Clearwire, a wireless broadband provider that has partnered with Bell Canada, has reserved the right to restrict access or terminate customers that use third party VoIP services.¹⁵ In Western Canada, Primus has said that its VoIP offering has been subject to spotty service from Shaw, a leading cable provider in B.C. and Alberta. Shaw is now offering a \$10 VoIP "quality of service enhancement" product accompanied by a warning that failure to pay the fee may result in quality of service issues with third party providers. Primus has objected, characterizing the fee as a VoIP tax.

VoIP represents an exceptionally important opportunity for the Canadian telecommunications marketplace as it has the potential to lower costs, increase services, and foster greater competition. From Internet-based services such as Skype to third-party services offered by companies such as Primus to the nascent offerings from Canada's traditional telecommunications providers, there is the potential for consumers to enjoy a dizzying array of VoIP services. The Canadian regulatory environment must provide for a level-playing field for all such offerings. In that regard, **telephone and cable broadband providers should be legally prohibited from configuring their networks to favour or preference their own VoIP offerings over the competition.** The treatment of "bits" should be equal and devoid of any preferencing such that emerging competitors can realistically compete with established providers.

III. INTERNET PRIVACY (Issue B31)

Canada's telecommunications framework must fully protect privacy for Internet-based activities. As Justice LeBel of the Canadian Supreme Court warned last summer, "monitoring of an individual's surfing and downloading activities...tend to reveal core

¹³ Canada, CRTC *Telecom Decision CRTC 2005-28: Regulatory framework for voice communication services using Internet Protocol*, (Ottawa: May, 2005), <<http://www.crtc.gc.ca/archive/ENG/Decisions/2005/dt2005-28.htm>>.

¹⁴ Madison River Communications, LLC: “Consent Decree” (3 March 2005), FCC DA 05-543A2 at 3, online: Federal Communications Commission <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf>.

¹⁵ Michael Geist "CRTC Picks Wrong Analogy in Net Telephony Ruling" *The Toronto Star* (May 2005), <http://www.michaelgeist.ca/resc/html_bkup/may162005.html>

biographical information about a person.”¹⁶ The sensitive nature of Internet usage data places ISPs in a particularly critical position as the guardians of that information. This became particularly apparent in the *BMG v. Doe* case, which involved Internet file sharing.¹⁷ The Federal Court of Appeal’s May 2005 decision emphasized the importance of online privacy protection, stating that “citizens legitimately worry about encroachment upon their privacy rights. The potential for unwarranted intrusion into individual personal lives is now unparalleled. In an era where people perform many tasks over the Internet, it is possible to learn where one works, resides or shops, his or her financial information, the publications one reads and subscribes to and even specific newspaper articles he or she has browsed.”¹⁸

While the court acknowledged the obvious – privacy rights are not absolute and must sometimes take a back seat to other interests – it proceeded to establish a rigorous test designed to provide significant privacy protections. The test requires a plaintiff to first demonstrate that it has a “bona fide” claim based on evidence that it has obtained (not merely that it intends to file a lawsuit) and that it has no other improper purposes for seeking the identity of the subscribers. The plaintiff must demonstrate that the information cannot be obtained from another source and tender evidence that is (i) admissible, (ii) timely, and (iii) links the Internet protocol addresses of the subscribers to the alleged infringement.

The importance of each of these evidentiary requirements should not be underestimated. In addressing the deficiencies of this particular case, the court warned that relying on faulty evidence created “the risk that innocent persons might have their privacy invaded and also be named as defendants where it is not warranted.”¹⁹

Assuming that the evidentiary hurdles are met, the test then requires courts to determine whether the public interest in disclosure outweighs the privacy interests that are at stake. If the court determines that disclosure is appropriate, it must ensure that privacy rights are invaded “in the most minimal way” such that the plaintiff must collect no more information than is necessary for the purpose of the claim. The court recommended that judges provide specific directions on how the information can be used and also consider keeping the information from the broader public by issuing a confidentiality order or identifying the defendants solely by their initials.

While Canadian courts have recognized the need to provide strong privacy protections for online conduct, Canadian telecommunications law features only limited protections. With courts recognizing the importance of Internet-based privacy, it is critical that the

¹⁶ *Socan* supra at 155.

¹⁷ *BMG Canada Inc. v. Doe*, 2005 FCA 193, < <http://www.canlii.org/ca/cas/fca/2005/2005fca193.html>>, [BMG],

¹⁸ *Ibid.* at 4.

¹⁹ *Ibid.* at 21

Canadian legal framework reflect the importance of protecting individual privacy. This can be best achieved **by statutorily permitting the disclosure of subscriber personal information only under court order** where the privacy interests of the individual can be fully considered and protected.

Moreover, Canadians should be informed when their personal information has been compromised due to a security breach at an ISP. The Act should therefore include a **positive obligation on ISPs to report breaches in the security of personal information in their possession**. Such a provision would be modeled after the State of California's SB1386, a two-year old law which mandates that companies and agencies that do business in the state or possess personal information of state residents must report breaches in the security of personal information in their possession.²⁰

The privacy associated with the Internet is not limited to private sector disclosure requests or breaches. The government's lawful access initiative poses a further privacy risk to Canadian Internet telecommunications. While the term lawful access sounds innocuous, the program, which dates back to 2002, represents law enforcement's desire to re-make Canada's networks to allow for lawful interception of private communications.

If lawful access becomes reality, Canada's ISPs will be required to refit their networks to allow for real-time interception of communications, to have the capability of simultaneously intercepting multiple transmissions, and to provide detailed subscriber information to law enforcement authorities without a court order within 72 hours.

Moreover, Canada's ISPs will be subject to inspections and required to provide the government with reports on the technical capabilities of their networks. All of these activities will be shrouded in secrecy with ISPs facing fines of up to \$500,000 or sentences of up to five years in jail for failing to keep the data collection confidential.

All of these changes come at an enormous cost – both financially (hundreds of millions of dollars in new technology) and to the personal privacy of all Canadians. While some changes may be needed for security purposes, the government has yet to make the case for why the current set of powers, which include cybercrime and wiretapping provisions, are insufficient. Moreover, there has been little evidence provided that this approach is the least privacy invasive alternative.

As in the private sector context, is essential that **for law enforcement purposes Canadian law ensure that subscriber information is only disclosed under court order**. Moreover, the policy framework should recommend that **Canadian networks adopt the least privacy invasive approach possible**.

²⁰ 2002 Cal SB 1386, < http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=0102&house=B&site=sen>

POLICY REFORM RECOMMENDATIONS (Issues G1, G5, G7)

The *Telecommunications Act* was not drafted with the Internet in mind, however, its stated objectives are broad enough to cover universal broadband access, legislated network neutrality, and Internet privacy. Section 7 of the Act identifies nine objectives. These include “reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada”,²¹ response to “economic and social requirements of users of telecommunications services”,²² and contribution to “protection of the privacy of persons.”²³

Although the telecommunications framework can accommodate Internet issues, significant reforms are still needed to implement these issues into Canadian law. Given the immediacy of these issues and the critical nature of full Canadian participation in the online environment, all of the reforms discussed below should be treated as a phase one or top priority reforms.

1. A new policy framework should be established to facilitate universal access to broadband much like policies of an earlier era ensured comprehensive local phone service. As noted above, **where cable and telephone providers have proven unwilling to offer commercial broadband services, federal, provincial and local governments should fill the void** to ensure that all Canadians enjoy access to e-commerce, distance education opportunities, tele-health, and e-government services. In fact, **even in communities with both cable and telco broadband choices, local municipalities should consider offering a third, publicly supported broadband alternative modeled after traditional utilities. The timeframe for such an initiative must also be a priority with the goal of universal broadband access to all Canadians by the end of 2008.**
2. In an era where growing convergence leaves Canadians with limited broadband choices and providers with economic incentives to favour their own (or affiliated content) over competing services or offerings, **content neutrality in the provision of network services is an absolutely essential principle that should be firmly established under Canadian law backed by regulatory oversight and significant penalties for compliance failures.**

²¹ Telecommunications Act, 1993, c. 38 s. 7 (b) < <http://www.canlii.org/ca/sta/t-3.4/sec7.html>>

²² *Ibid.* at s. 7(h)

²³ *Ibid.* at s. 7(i)

The issue of network neutrality is not limited to content. It is also a core principle in the availability of applications running on the network. A current example in this regard involves VoIP services. In that regard, **telephone and cable broadband providers should be legally prohibited from configuring their networks to favour or preference their own VoIP offerings over the competition.** The treatment of “bits” should be equal and devoid of any preferencing such that emerging competitors can realistically compete with established providers.

3. The Act’s privacy provisions require updating since they focus on traditional phone services. The new provisions should establish strong privacy protections for all Canadian Internet users including a **prohibition on disclosures of personal information, including Internet-based activities, without judicial oversight.**

Moreover, the Act should include a **positive obligation to report breaches in the security of personal information in their possession.** Such a provision would be modeled after the the State of California’s SB1386, a two-year old law which mandates that companies and agencies that do business in the state or possess personal information of state residents must report breaches in the security of personal information in their possession. Companies are required to act quickly, notifying customers in writing, electronically, or by prominently posting the information on their website.

The California law has spawned nearly a dozen imitators throughout the United States as other states seek to provide their residents with similar protections. Moreover, pressure has begun to build on the U.S. Congress to adopt a national reporting law to provide all residents with equal treatment and to ensure that all companies face a single nationwide standard.