Public Comments for CRTC Interrogatory PN 2008-19

Prepared by Christopher Parsons[*]

Summary: This document identifies privacy concerns surrounding the use of Deep Packet Inspection (DPI) devices by Canadian Internet Service Providers (ISPs). After outlining some of these concerns, I note ways that DPI can be used in to minimize privacy risks.

February 22, 2009

[*] Doctoral student in the University of Victoria's Political Science department.

Table of Contents

Introduction

The Canadian Radio-television and Telecommunication Commission (CRTC) has initiated a public proceeding to consider the Internet traffic managing practices that Canadian Internet Service Providers (ISPs) employ to govern network link congestion. This proceeding is meant to clarify what practices are, and are not, appropriate for managing Canadians' Internet traffic. This author's contribution to the process examines the impact of Deep Packet Inspection (DPI) technologies on Canadians' privacy. After briefly outlining the capacities of DPI technologies, I suggest that their ability to examine the content of packets poses a privacy risk and, consequently, falls under the CRTC's purview as part of the *Telecommunciation's Act*, Section 7(i). After providing a series of examples and reasons for why DPI technologies may invade Canadians' privacy, I conclude by suggesting ways of deploying DPI to avoid infringing/mitigate infringements on Canadians' privacy.

Overview of Deep Packet Inspection

DPI technologies enable network operators, such as ISPs, to examine the payloads of data packets that their customers transmit to, and receive from, the Internet. Using these devices, ISPs can "look inside all traffic from a specific IP address, pick out the HTTP traffic, then drill even further down to capture traffic headed to and from Gmail, and can then reassemble e-mails as they are typed out by the user" (Anderson 2007). DPI devices are designed, in part, to defeat obfuscation techniques that some applications use to mask packet contents by drilling past header information and into the packet payload.

Even when consumers encrypt their data traffic it is possible to identify the applications responsible for sending and receiving data packets because DPI devices are often integrated with 'Deep Flow Inspection' (DFI) technologies. DFI lets network operators identify the applications that are responsible for sending and

receiving data packets from the Internet; it evaluates the spikes and bursts of encrypted web traffic, as well as ports used, to correlate traffic patterns with those unique to particular programs (Finnie 2009). As a result, it is possible to identify applications generating data traffic, even when the application (e.g. Skype, Bit Torrent) actively attempts to subvert packet surveillance (Bonfiglio, Mellia, Meo, et al. 2008).

Benefits of Deep Packet Inspection for Network Operators

By examining packet flows at detailed levels, ISPs can improve network security and guarantee different levels of service to various customer-types. Network security is improved because system administrators can correlate particular packet exchanges with worm- and virus-like behavior, and implement measures to automatically quarantine infected devices from the rest of the ISP's network. Different levels of service can be guaranteed by associating particular application-types with particular usage-plans or priority levels; a user on a VoIP plan might have their VoIP packets prioritized, whereas a user with a Bit Torrent plan might have their Bit Torrent packets given priority on the network. Alternately, all individuals may be given the same plan, and simply have some packets prioritized and others deprioritized. I am unaware of any 'application-type' service plans being provided in Canada at the moment, though DPI devices *are* being used to prioritize or de-prioritize packets based on the application that is found generating them.[1] From the ISP submissions for Public Notice 2008-19, one can generally say that DPI-enabled ISPs *are* prioritizing latency sensitive applications, such as VoIP, and de-prioritizing what they have identified as 'time insensitive' applications, such as P2P applications. Further, many ISPs are targeting P2P applications, even when links are not experiencing congestion, to preemptively address the possibilities links becoming congested. P2P has been stated as the dominant reason why ISPs are deploying DPI devices to manage network traffic.

Privacy Implications of Deep Packet Inspection Devices

Pursuant to the *Telecommunications Act*, Section 7 (i), it is important that the Commission evaluate whether DPI devices will "contribute to the protection of the privacy of persons." I suggest that these devices will not contribute to the protection of Canadians' privacy, and instead threaten to upset traditional privacy protections that Canadians have come to expect when communicating with one another. On the basis of this, I will argue that ISPs must make changes in how they implement DPI technologies on their network.

---

[1] It should be noted that ISPs in the United States of America, such as Comcast, have adopted an 'application agnostic' throttling system, whereby any user who sustains their maximum bandwidth rate for a certain period (regardless of application) subsequently has all of their bandwidth throttled for a period of time. This is meant to address concerns that throttling particular application-types is a violation of network neutrality principles, as well as to respond to consumer complains about application-targeted throttling.

Privacy, when understood as a state that is free from external obtrusions or disturbances, conjoins a series of interrelated though distinctive privacy classifications: freedom to control one's personal information (informational privacy); freedom to isolate oneself (accessibility privacy); and freedom to speak and associate with others (expressive privacy) (Parsons 2007). As a value, privacy is often 'sacrificed' to other interests – interests of security, of profit, of convenience (Bennett 2008, Solove 2008, Torpey 2000) – but in the present proceeding, such a sacrifice would have deep impacts on the lives of Canadians. To constrain this discussion, I will primarily focus on how DPI threatens Canadians' expressive privacy.

Judith Wagner DeCew, a noted privacy and legal theorist, has noted that even "surveillance of normal, everyday activities can lead one to be distracted and feel inhibited" (Wagner DeCew 1997: 76). Julie Cohen argues that "[P]ervasive monitoring of every move or false start will, at the margin, incline choices toward the bland and mainstream." Broad-based surveillance, such as the ubiquitous examination of packet streams by ISPs, thus "threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it" (Cohen 2000: 1426). This view is shared by Paul Schwartz (2000), psychoanalysts Donald Winnicott (1965) and R.D. Laing (1967), as well as by privacy and surveillance scholars Daniel Solove (2008) and David Lyon (2008). Further, security experts Susan Landau and Whitfield Diffie have argued that the introduction of broad-based surveillance technologies into contemporary packet-based network architectures fundamentally endangers citizens' privacy and raises the specter of vast security risks (Diffie and Landau 2007, Landau 2006).

ISPs who admit to using DPI equipment for parsing data packets are using equipment that can examine the payload of packets, or the portions of packets that contain content information of communications. Thus, network operators can examine "Layer-7" of packets, which lets them identity the actual messages that are sent by programs such as Internet Explorer, MSN, or Microsoft Outlook. ISPs who are involved in the CRTC's proceeding have stated that they do not examine the actual content of packets and that they have no commercial interest in doing so. While stating this, we see Bell acknowledging that they *do* examine the Application layer (Layer-7) of packets, the layer holding payload content. Further, Rogers presently modifies users' data content using their DPI technologies (which will be discussed in more length shortly). With the exception of Shaw (who maintain that they are using Arbor-Ellacoya equipment to only examine packet headers), most Canadian ISPs using DPI devices are already examining packets' Layer-7. They *are already* reading the 'content level' of data transmissions in determining what application is sending and receiving data packets from the Internet, and in at least one case are actively modifying those transmissions.

While surveying the application-type that consumers are using to communicate arguably does not constitute a violation of individuals' privacy, consumers would not know if by intent or accident an ISP were to record its customers' data-content.

Digital communications are increasingly used by Canadians, and are replacing the analogue technologies that they have historically used; email is replacing written letters, instant messages and VoIP replace telephone conversations, and uploading videos to YouTube rather than inviting friends over for a vacation slide show is increasingly normal. These historical, analogue, technologies enjoyed relatively robust privacy protections under Canadian law, and Canadians' digital communications should be similarly safeguarded – technologies that would invade the privacy provided by analogue devices should be critically examined. Any suggestion that all mail should be examined for content-type by the post office before it is delivered, or that all phone conversation traffic should be persistently monitored though not recorded in the name of managing network congestion would be met with scorn by Canadians, at best. A similar degree of privacy protection should be encoded into the regulations for the digital communicative sphere. Analogue mail systems and telephone networks alike have had to address congestion challenges in their lifetimes, but this has not meant that postal outlets or telecommunication providers have been generally permitted to inspect the contents of messages and prioritize particular communications-types over others. Doing so would have been a massive privacy invasion of the individuals engaged in communications with one another. If ISPs are permitted to examine the application-layer of packets then consumers will be forced to communicate with one another knowing that there is a persistent possibility that their ISP could be engaging in ubiquitous surveillance by accident or malicious intent. Wagner DeCew and Cohen, as previously mention, recognize persistent and ubiquitous surveillance can result in substantial harms to how the surveyed communicate with one another.

Even were Canadians to encrypt their data traffic to shield themselves from the possibility of content-based surveillance, DFI technology lets ISPs determine the particular applications that Canadians use, and throttle particular packets based on their originating application – encryption does not entail an avoidance of ISP surveillance. Together, DPI and DFI allow ISPs to perform a level of granular surveillance that has historically been limited by technical and infrastructure limitations along with legal strictures.

Injecting Content with DPI – Rogers as a Case Model

It should be noted that none of the publicly filed comments from Rogers mentioned their use of DPI devices to modify their consumers' data traffic. Rogers have used DPI to 'splice' messages into users' data-streams as a facet of managing network congestion; when users approach their monthly bandwidth allotment a message is inserted above web pages that customers browse to, and informs them that they are reaching the allotted bandwidth (Stirland 2007). Rogers customers cannot *prevent* Rogers from inserting these messages into unencrypted data traffic streams, though they are given an opportunity to opt-out of such content injections after receiving their first message. Figure 1 provides an example of what these messages look like.

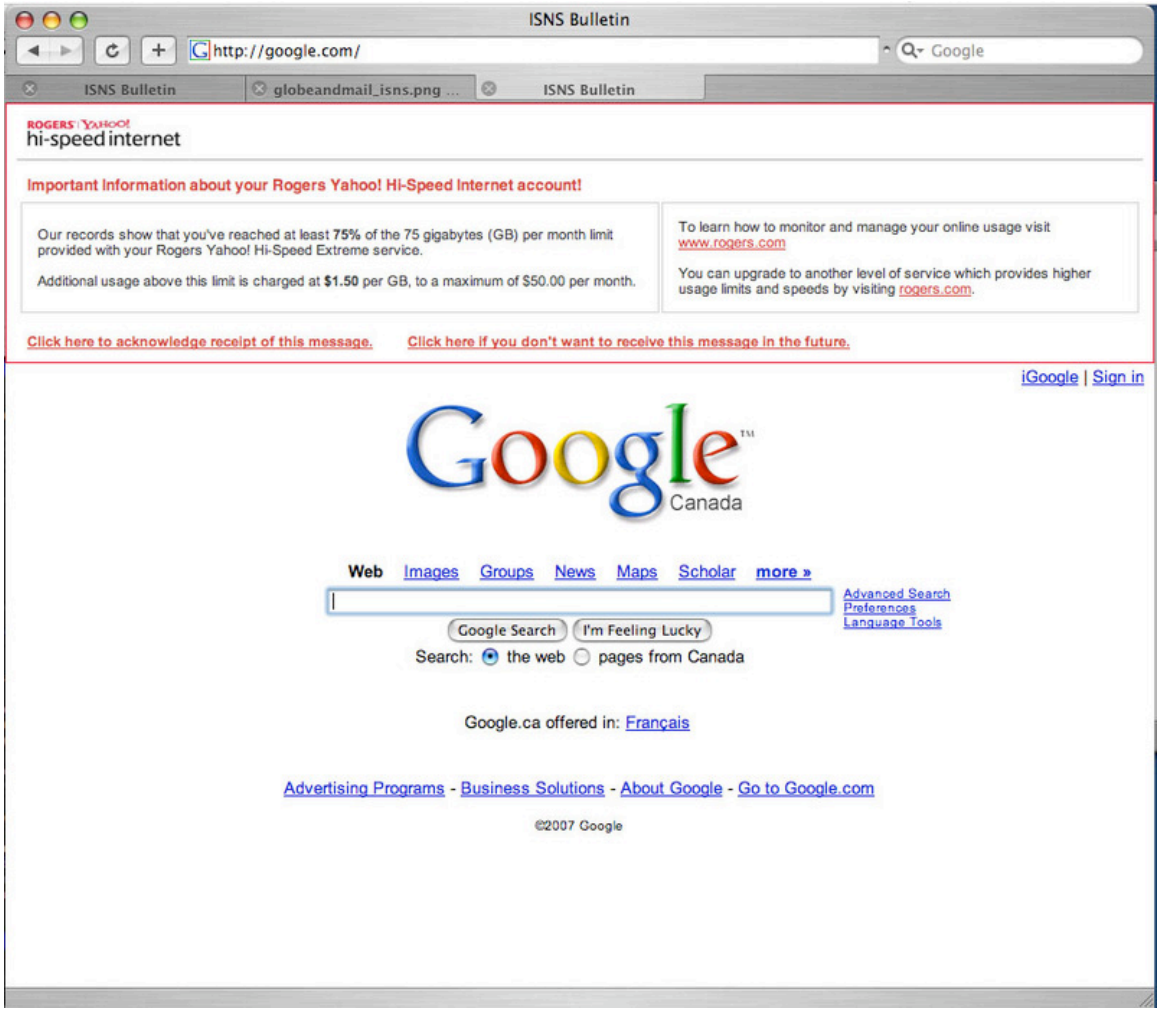

Figure 1: Example of Rogers' Injected Content (Weinstein 2007)

As is demonstrated from this figure, Rogers uses DPI devices modify web pages, and even Internet companies such as Google are helpless to prevent it. While the notice from Rogers appears benevolent and has been defended by Rogers' vice president of communications, Taanta Gupta, as a way of improving communication between Rogers and their customers (Stirland 2007), the benefits of this injection do not mitigate the method used by Rogers to 'alert' their customers; Rogers is effectively performing a 'man-in-the-middle' attack. Rogers' exploitation of their DPI equipment to modify content demonstrates that they *are* interested in their customers' data content (e.g. HTTP web pages) for the purposes of education-oriented bandwidth-management. Rogers is not interested in maintaining 'dumb pipes'.

Reviewing Privacy Implications

The discussion thus far demonstrates how DPI threatens to undermine the privacy and security of users' communications; such network management technologies open the possibility for surreptitious surveillance and/or alteration of content presented to end-users. End-users are unlikely to ever be aware of the surveillance,

or subtle content alterations, of their data traffic, and even if they encrypt the totality of their data traffic DFI still subjects them to pervasive surveillance. Diffie and Landau's comments about the risks engendered with ubiquitous surveillance of Internet communications ring especially true in the case of ISPs deploying DPI, where a security breach could let third-parties survey and/or alter Canadians' data traffic on either a massive or a specific scale. Introducing DPI and DFI that inspects the application layer of packets into network operators' operations creates a substantial possibility for widespread infringement on Canadians' personal communicative privacy.

In summary, DPI technologies endanger Canadians' privacy because it is a technology that can examine and/or analyze the entirety of Canadians' non-encrypted data that is sent to, and received from, the Internet. This is not to suggest that ISPs are presently using the technology to cache Yahoo! messenger messages, or the video and voice data transmitted using VoIP applications, but at least one Canadian ISP has demonstrated a willingness to use DPI to modify the contents of web pages. The shift to analyzing data content (and in some cases modifying it), as well as dynamically altering transmission bandwidth available to particular applications is a radical shift from the stance of ISPs as common carriers who transmit data traffic with little regard to its content. Previously, only in cases of emergency were particular communications traffic (e.g. police, fire) given priority over other communications – what was once exceptional in the sphere of analogue communications threatens to become the norm in the sphere of digital transmissions.

Using DPI Non-Invasively

Shaw is presently using DPI devices to solely examine data packets' header information – as placed on the public record, Shaw's devices are not collecting any more data than is normally required to deliver packets to their destination. Were all Canadian ISPs to use their equipment similarly, their usage of DPI could not be reasonably considered to invade Canadians' privacy any more than typical data routing equipment. It is when ISPs actively penetrate the payload, and in particular Layer-7 of packets, that concerns related to privacy arise. By reconfiguring DPI devices to *avoid* analyzing packets' Layer-7, as well as to *avoid* or *stop* modifying consumers' data traffic, many of the privacy issues surrounding DPI devices could be mitigated.

If this method of packet analysis is unsuitable for managing network congestion, then ensuring that customer's personally identifiable information is clearly segregated from data packet streams is the next-best option. This is already a process that occurs in Bell's system, where customers' personal information (e.g. name, age, etc) are divorced from their customer identification number. As outlined by Bell, their DPI equipment does not correlate personal information with the consumer identification number, and thus cannot discriminate towards or against particular customers based on personal information. If Canadian ISPs deploy policy control and management appliances bundled with DPI and DFI technologies – as

Finnie (2009) suggests is on the horizon – it will be important for these appliances to *continue* separating personally identifiable subscriber information and packet analysis heuristics and their logs.

Even when adopting this latter path to alleviate some privacy concerns concerning the association of personally identifiable information and network management technologies, the underlying security challenges and accompanying privacy risks introduced by integrating DPI and DFI into ISP networks would be left unaddressed. Diffie and Landau's concerns would remain.

Conclusion

Canadians are increasingly turning to digital mediums to communicate with one another, to pursue opportunities for self-education, and to engage in intimate relationships. Actions and expressions that took place in analogue environments are increasingly being virtualized, and it is important that in determining appropriate network management techniques and practices that the freshness of the digital does not overwhelm existing regulations concerning appropriate levels of surveillance and analysis of Canadians' communications. Per the *Telecommunications Act*, new communication technologies are expected to "*contribute* to the protection of the privacy of persons" (emphasis added) – DPI technologies, when used to examine the application layer of packets, do not contribute to, and in fact erode, Canadians' privacy protections. On this basis, should DPI devices be seen as an acceptable technology for managing network congestion, they must be configured in such a way to avoid examining the content of Canadians communications. Doing otherwise would *detract* from the protection of the privacy of persons, and stand in opposition to the *Telecommunications Act*.

Reference

Anderson, Nate (2007). "Deep Packet Inspection meets 'Net neutrality, CALEA," *ArsTechnica*. Published July 25, 2007. Last accessed October 10, 2008. Accessible at: http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars

Anderson, Nate (2008). "Comcastic P4P trial shows 80% speed boost for P2P downloads," *ArsTechnica*. Published November 3, 2008. Last accessed February 14, 2009. Accessible at: http://arstechnica.com/old/content/2008/11/comcastic-p4p-trial-shows-80-speed-boost-for-p2p-downloads.ars

Bangeman, Eric (2008). "Rogers latest ISP to "Help" customers with DNS redirects," *ArsTechnica*. Published July 20, 2008. Last accessed February 18, 2009. Accessible at: http://arstechnica.com/news.ars/post/20080720-rogers-latest-isp-to-help-customers-with-dns-redirects.html

Bennett, Colin (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, Mass.; The MIT Press.

Bonfiglio, Dario, Marco Mellia, Michela Meo, Dario Rossi, and Paolo Tofanelli (2007). "Revealing Skype Traffic: When Randomness Plays With You," *Computer Communications Review*, vol. 37(4), pp. 37-48.

Cohen, Julie (2007). "Examined Lives: Informational Privacy and the Subject as Object," 52 Stanford Law Review 1373.

Diffie, Whitfield, and Susan Landau (2007). *Privacy On the Line: The Politics of Wiretapping and Encryption*. Cambridge, Mass.: The MIT Press.

Finnie, Grahm (2009). "ISP Traffic Management Technologies: The State of the Art." Last accessed February 18, 2009. Available at: http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm

Laing, R.D. *The Politics of Experience*. New York: Ballantine Books.

Landau, Susan (2006). "National Security on the Line," *Journal of Telecommunications and High Technology Law*, vol. 4 (2), pp 409-447.

Lyon, David (2008). *Surveillance Studies: An Overview*. Malden, MA: Polity Press.

Parsons, Christopher (2007). "Technology, Communication, and Western Pluralistic Democracies: Aligning Digital Privacy to Facilitate Citizen-Solidarity." (Masters Thesis). Last accessed: February 18, 2009. Available at: http://www.christopher-parsons.com/Thesis/Technology_Communication_and_Western_Pluralistic_Democracies(for_web).pdf

Schwartz, Paul M. (2000). "Privacy and Democracy in Cyberspace." Last accessed February 15, 2009. Available at SSRN: http://ssrn.com/abstract=205449

Solove, Daniel J. (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.

Stirland, Sarah Lai (2007). "In Test, Canadian ISP Splices Itself Into Google Homepage," *Wired Threat Level (blog)*. Published December 10, 2007. Last accessed February 18, 2009. Accessible at: http://blog.wired.com/27bstroke6/2007/12/canadian-isps-p.html

Torpey, John (2000). *The Invention of the Passport: Surveillance, Citizenship and the State*. Cambridge, UK: Cambridge University Press.

Wagner DeCew, Judith (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithica, New York: Cornell University Press.

Weinstein, Laura (2007). "Google Hijacked – Major ISP to Intercept and Modify Web Pages," *Laura Weinstein's Blog*. Published December 8, 2007. Last accessed February 18, 2009. Accessible at: http://lauren.vortex.com/archive/000337.html

Winnicott, Donald (1965). *The Maturational Processes and the Facilitating Environment: Studies in the Theory of Emotional Development*. New York: International Universities Press.

Whitt, Richard (2008). "Net neutrality and the benefits of caching." Google Policy Blog. Posted December 15, 2008. Last accessed February 14, 2008. Available at: http://googlepublicpolicy.blogspot.com/2008/12/net-neutrality-and-benefits-of-caching.html