What's Driving Deep Packet Inspection in Canada?

ISPs, netscapes of power, and privacy advocacy

By Christopher Parsons[*]

Abstract: Canadian ISPs are developing contemporary netscapes of power. Such developments are evidenced by ISPs categorizing, and discriminating against, particular uses of the Internet. Simultaneously, ISPs are disempowering citizens by refusing to disclose the technical information needed to meaningfully contribute to network-topology and packet discrimination discussions. Such power relationships become stridently manifest when observing Canadian public and regulatory discourse about a relatively new form of network management technology, deep packet inspection. Given the development of these netscapes, and Canadian ISPs' general unwillingness to transparently disclose the technologies used to manage their networks, privacy advocates concerned about deep packet networking appliances abilities to discriminate between data traffic should lean towards adopting a 'fundamentalist', rather than a 'pragmatic', attitude towards these appliances. Such a position will help privacy advocates resist the temptation of falling prey to case-by-case analyses that threaten to obfuscate these device's full (and secretive) potentialities.

June 28, 2009
Draft Version :: 1.3

[*] Doctoral student in the University of Victoria's Political Science department and member of the New Transparency Project. Thanks to the participants of the Infoscape June 18, 2009 Roundtable for comments. Funding to pursue this research is provided by a SSHRC fellowship as well as by the New Transparency Project. Comments welcomed, email to Christopher@christopher-parsons.com

Table of Contents

Introduction **1**

I – What is DPI? **2**

What are the advantages of DPI over earlier packet inspection technologies? **3**

What is significant about looking at the application-layer? **4**

II – How do Canadian ISPs claim DPI is being used? **6**

ISPs on the public record **6**

III – Techniques of obfuscation, avoidance, and refutation **11**

Network Architecture and Walled Gardens **11**

Private Knowledge **15**

IV – The Fundamentalist Approach **16**

The Activist/Fundamentalist **16**

The Pragmatist **17**

Canadian Privacy Advocacy and DPI **18**

Conclusion **19**

Works Cited **20**

Introduction

Canadians are prolific users of YouTube, principle members of the 'Facebook nation', and are increasingly taking to online environments to protest government and corporate behaviour. They now spend an estimated 40% of their leisure time one (Shaw 2008). In light of a recent CRTC investigation into how Canadian ISPs manage bandwidth, it appears as though there is a substantial cost for enthusiastically embracing online services: traffic management practices. These practices often entail the use of Deep Packet Inspection (DPI) networking appliances to 'protect' telecommunications infrastructure from packet congestion that threatens to slow or end Canadians' access to the Internet. ISPs maintain that remaining digitally connected to the world requires that data sent to and received from the Internet be tightly monitored and regulated, or else it will be the end of the Internet as we have become accustomed to it.

The death of the Internet is something that we have been warned about for some time. Bret Swanson at the Discover Institute prepared a piece titled "The Coming Exaflood" (2007) to warn that, if the Federal Communications Commission does permit ISPs to engage in bandwidth discrimination, or at least let them charge content providers to transmit their content, the Internet will collapse as ISPs are unable to shuttle data packets across the Internet at the rate that they are generated at. The Internet Innovation Alliance (IIA) has prepared similar prognoses (IIA 2007). In the case of Swanson and the IIA, they are rehearsing Bob Melcalfe's arguments that "gigalapses" are coming (Melcalfe 2006).

The catch? Melcalfe was writing in 1996.

In effect, the end of the Internet has been talked about for so long that fair quantities of *paper*, as well as bits and bytes, have been sacrificed to warn us of the oncoming deluge of data traffic. To manage this digital flood, like dams manage water, ISPs argue that they must use increasingly sophisticated network appliances to control the flow of data by heuristically identifying likely packet-types and associated applications. Having done so, they argue that rules must be applied to data traffic, to dynamically control packet transfer speeds; they need to use rules to raise or lower the data flood-gates. Some (though certainly not all) of these DPI network appliances 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). In effect, these are incredibly powerful devices, and they are being broadly deployed across network infrastructures throughout Canada.

In this paper, I argue that Canadian ISPs are deploying DPI appliances in a way that propels what Winsek has termed 'netscapes of power'. In such netscapes, network topologies empower ISPs to categorize and discriminate against particular uses of the Internet while disempowering citizens by withholding technical information that citizens require to meaningfully contribute to network-topology and filtering discussions (Winseck 2005). As a result of these netscapes, and ISPs' general unwillingness to transparently disclose the technologies used to manage their networks, privacy advocates should lean towards adopting a 'fundamentalist' rather than a 'pragmatic' attitude towards uses of DPI network appliances to avoid the temptation of falling prey to case-by-case analyses that may obfuscate these device's potentialities.

To advance this argument, I first discuss how DPI appliances broadly work, and why they are an innovative and significant shift from earlier packet analysis techniques. I then turn to discuss public comments recently filed to the CRTC about how ISPs use DPI appliances. Here, I substantiate some of the earlier discussions of DPI to clarify how these technologies are actually being used by Canadian ISPs and what ISPs claim is driving their deployment. This done, I turn to address netscapes of power, and specifically point to instances where ISPs have both refused to publicly provide information about their network technologies and the perceived impact of this lack of information by consumer groups. I conclude by arguing that, in the absence of fully transparent public statements on how Canadian ISPs are using DPI appliances, privacy advocates would be well advised to take more of a 'fundamentalist' than a 'pragmatic' approach to DPI. This stance is warranted on the basis that pragmatic approaches demand familiarity with devices' technical capacities, whereas fundamentalist positions reserve broader theoretical and epistemological resources for argumentation and discourse.

I – What is DPI?

Deep Packet Inspection (DPI) is a broad term given to networking technologies that can heuristically engage with packets on the basis of the application or application-type that has generated, or is receiving, packets by examining the totality of a packet. This degree of inspection is qualitatively and quantitatively superior to earlier modes of packet analysis, and thus represents a significant shift in the extensiveness of packet surveillance. In this section, I distinguish DPI appliances from earlier network inspection technologies, and briefly describe the significance of classifying data traffic according to application-type. Having outlined the advertised (typically referred to 'theoretical') capacities of DPI network appliances, we will turn to address how and why Canadian ISPs claim to be deploying them in their own networking environments.

What are the improvements of DPI over earlier packet inspection technologies?

Packet inspection technologies are a required element of network topologies, just as wings are necessary for planes to fly. However, just as plane wings have become more efficient in carrying aircraft over the past century, network inspection technologies have become more efficient and sophisticated in analyzing and mobilizing packets across network topologies.

Earlier inspection technologies can be broadly referred to as Shallow Packet Inspection (SPI) or Medium Packet Inspection (MPI). SPI technologies typically encompass most rudimentary firewalls (e.g. that built into Windows XP) and apply preset rules to packet that are trying to enter or exit a client computer.[1] Such technologies often rely on simply refusing to pass packets along, and while some can keep detailed logs of packet transactions, these logs are based only on information that is gathered from packets' header, or routing, information (per the OSI model). This means that the payload, or content, of the packet escapes inspection by SPI devices, though packet transfer analysis does offer these technologies the ability to discriminate against packets based on their flow characteristics.

MPI technologies are often embedded in what are termed 'application proxies', which are networking appliances that stand between an end-user's computer and the Internet-at-large. These proxies are often placed inline with ISPs' networking equipment, and tend to use parse-lists to examine the destination and origin of a packet (based on IP-address), as well as some data formats. Further, these devices can prioritize some packets over others by examining the commands in the application layers, and can also examine the file formats that are exhibited in the presentation layer (Porter et. al. 2006). The difficulty with these devices is that they suffer from incredibly poor scalability. Every application protocol that is examined requires a separate application gateway, and inspections necessarily increase packet latency (Tobkin and Kligerman 2004). These latter two limitations make these appliances of limited use in large networking environments.

DPI appliances offer superior scalability to MPI devices, and are better able to examine Layer-7 traffic, or the payloads of data packets. One manufacturer,

[1] It does have to be noted that some firewalls with intrusion detection systems are intended to penetrate the application-layer of a packet in order to evaluate content. Firewalls such as this exceed the definition of 'rudimentary' firewalls. For more: http://www.securityfocus.com/infocus/1716

Arbor/Ellacoya, recognizes that these devices can penetrate layers 3-7 of data packets and provide network operates with "crucial information to your operations and business support systems, without compromising other services" (Arbor/Ellacoya Networks 2008). Further, many of these appliances can be rapidly reconfigured, enabling administrators to update inspection protocols with relative ease; this is a selling feature of the Ipoque's PRX-10G, which is advertised as including regular signature updates, which lets ISPs identify emerging data transfer protocols and apply rule sets accordingly (Ipoque 2008). While DPI is a natural *progression* of packet inspection, as a progressive technology it has not left earlier packet inspection devices' unique capabilities behind.

Where it is impossible to analyze a packet's application-or-origin, typically because of encryption, a set of packets can be captured to understand their originating application. Deep Packet Capture (DPC) technologies, which are often built into DPI appliances, copy unlabelled packets to a local processing unit. This unit attempts to determine the signature of the packets, which "is usually possible within the first few packets in a flow, but upon occasion 50-100 packets are required" (Unions des Consommateurs 2009). This helpful because it lets network administrators 'get around' the problem of packet payload encryption, which defeats DPI analysis on its own.[2] In cases where neither DPI nor DFC approaches are sufficient for understanding what application a packet belongs to, heuristic analyses of packet transfers are applied and cross-referenced with already known packet exchanges to determine the program generating or receiving the packet(s). In the case of Skype, which is well known for obfuscating *and* encrypting its traffic, a DPI appliance would look for the very particular way that packets are exchanged between participants on the call and their sizes. Using information such as "payload lengths, number of packets sent in response to a specific transaction, and the numerical offset of some fixed string (or byte) value within a packet" lets network administrators identify what application is transferring the packets and apply their rule sets (Allot 2007). Encryption, what was widely considered a substantial antidote to digital surveillance in the 90s, can no longer be considered the sole antidote to packet surveillance and predictive content analysis that are found in contemporary network topologies.[3]

What is significant about looking at the application-layer?

While Anderson's earlier comments (DPI as capable of drilling down all the way to a particular Gmail session) might seem a bit over the top, turning to the descriptions

[2] Encrypting the payload is intended to limit the capacity for intrusive understanding of packets' contents. Unions des Consommateurs has noted, however, that the "use of encryption does not guarantee that a flow will remain unclassified. If the encryption procedure is not executed carefully, then unintended signatures can remain (for example, the encryption procedure in Winny involved a detectable key exchange)" (2009).

[3] Of course, there are other issues concerning privacy when packet encryption is used. Diffie and Whitfield note in *Privacy on the Line* (2007) that a community's social relations can be mapped by simply watching encrypted traffic without ever needing to capture the content of the communications.

that DPI manufactures provide of their devices confirms their range of potential use situations. Bivio and Solera Networks claim that their devices let administrators, determine "the real causes of network problems, identify security threats, and ensure data communications and network usage complies with outlined policies" (2008). iPoque has released whitepapers detailing aggregate consumer use of ISPs' networks across Europe (iPoque 2009a) and the capacities for DPI to stop copyright infringement before full data transfers can be completed (iPoque 2009b). iPoque's whitepapers reveal the granularity of analysis that can (and does) take place in networks using their devices. Further, the behavioral advertising company Phorm, which relies on DPI, argues that their "technology enables comprehensive user targeting and real-time campaign optimisation. Phorm provides the ideal contextual and behavioural solution for advertisers and agencies worldwide. "[4] Moreover, the Campaign for Democratic Media recognized, when examining a submission by Arbor/Ellacoya to the CRTC's proceeding on Internet Service Providers' bandwidth management practices (PN 2008-19), that Arbor's technologies "can be used to prioritize traffic and time-shift file sharing into off-hours [which lets ISPs] save millions of dollars in capital expansion costs that would be necessary to meet growing bandwidth demands even without new subscriber acquisition" (Arbor Communications, in CDM 2009a). Beyond targeting particular application-types (e.g. Bittorrent), some devices can identify TOR traffic as well as recognize and adjust bandwidth for Flash, MMS, MPEG, World of Warcraft, and so on (Ipoque 2008). Effectively, while only a handful of devices are focused on the level of analysis that Anderson ascribes to Narus' appliances, the devices generally allow for analysis of data traffic that significantly exceeds what network administrators could engage in using SPI or MPI network appliances.

In essence, the transition to application-layer level analyses of data traffic enables ISPs to (more) effectively perform the following:

1. Engage in lawful interception tasks/surveillance operations as mandated by police and intelligence communities.
2. Regulate content and enforce copyright.
3. Manage bandwidth by limiting the use of 'problem' applications and more precisely manage subscriber access to services and bandwidth.
4. Enhance network security by using heuristics to watch for aggressive/harmful network activity.
5. Facilitate vertical integration by discriminating against particular services in favor of others.
6. Use behavioral advertising to monetize citizens' web browsing and application-use habits (Bendrath 2009).

Each of these actions is facilitated or enhanced by examining the application-layer of packets to determine what is responsible for transmitting the packets. It is valuable to note that there are different drivers for each of the above listed uses of DPI

[4] http://advertising.phorm.com/advertisers.php

technologies; we might charitably take Canadian ISPs at their word when they state that *they* have no interest in the content of information flowing across their networks, and are instead concerned in network congestion. Once these devices are integrated into a network topology, however, there is a worry that function creep will occur. As will be evidenced in the next section as we focus on Canadian ISPs exclusively, the use of DPI in Canada to throttle traffic is, itself, the result of function creep. As such, Canadians would be right to worry that function creep could continue as these appliances are ubiquitously deployed within Canadian ISP networks.

II – How do Canadian ISPs claim DPI is being used?

Having outlined the range of potential uses of DPI appliances it may seem as though citizens in a contemporary democracy might worry that these devices are 'surveillance instruments' or 'privacy invasive' on the basis that they can examine the application layer of packets. Before advancing this claim, let us see how these devices are actually being deployed in Canada, and how this may mediate our understanding of their present capacities. I will focus on how key players in the Canadian telecommunications industry have identified why their devices are deployed by relying on their public comments submitted during the CRTC's traffic management proceeding. Following this, I will speak to which of these practices conform to the above listed six uses of DPI, and thus how DPI is presently being applied in the contemporary Canadian telecommunications market. This will prepare us to move onto a discussion of how DPI is implicated in emerging netscapes of power, and the approachs that Canadian privacy advocates should adopt in relation to these networking appliances.

ISPs on the public record

Let us begin by noting which large Canadian ISPs have either formally stated they are using DPI appliances, or can be inferred to be using them based on analyses of how their consumers currently experience their Internet use. These ISPs include: Bell Aliant Regional Communications, Cogeco Cable Canada, Rogers Cable Communications, Shaw Communications, Saskatchewan Telecommunications,[5] and Bragg Telecommunications. What is perhaps most significant about this group is that they constitute Canada's dominant carriers; they are responsible for leasing lines to smaller 'downstream' ISP. Where network owners are using DPI for Internet Traffic Management both their own retail, as well as wholesale, customers are often affected by the management techniques (Rogers, as an example however, does not throttle their wholesale traffic).

[5] While SaskTel does admit to using Arbor Peakflow SP product, they use the appliances exclusively for detecting, analyzing, and mitigating network anomalies related to DDoS attack, botnets, and so forth rather than for broader traffic management purposes (Saskatchewan Telecommunications 2009).

These Canadian ISPs predominantly use DPI to limit the use of P2P file transfer programs and, at least in Bell's case, for subscriber management.[6] P2P programs open multiple TCP sessions simultaneously, and tend not to respect TCP slowdown requests. They are accused by all major ISPs as being a major cause of network congestion. On this basis, the formal argument that is presented by network operators is that 'fairness' and 'just delivery of services' requires ISPs to throttle disruptive packet-flows. Cogeco has gone so far as to argue that if they *did not* discriminate against P2P traffic they would effectively be favoring the users of P2P applications over non-P2P users (Cogeco 2009a).

Bell bases their decision to use DPI on finances and technology, maintaining that while "the Companies may explore a more granular application of bandwidth management in the future, the management tools that would be economically and technologically suitable for a telephone company using DSL network equipment to perform network management at the level of granularity and in the dynamic fashion suggested by some are not presently available in the market" (Bell 2009a). In other words, because DPI appliances are backward compatible with older networking equipment in Bell's hubs and can be integrated with more contemporary equipment, DPI is a preferred option based on the economic and technological realities of their situation. In a similar vein, Shaw maintains that it is uses DPI for efficiency reasons; Shaw is not interested in censoring or watching the contents of packets for the following reasons:

- Traffic management is about network efficiency, and nothing else.
- Shaw has nothing to gain in censoring or watching content because it is not an agent of the state.
- It is not technically possible to massively inspect content, and even if an ISPs such as Shaw were to do this they would quickly lose their customer base.
- Any act of massive content-based surveillance would be in contradiction of the telecommunications act (Shaw 2009).

Again, we see a Canadian ISP focus on market logics as driving the integration of DPI appliances into networking hubs, rather than a desire to massively monitor content transactions that Canadians are engaging in. In addition, DPI is useful for adjusting customers' normative expectations of 'good' and 'bad' uses of bandwidth. Cogeco implicitly sees this technology as part of a long-term 'training' of consumer behavior when they refer to the inadequacy of usage billing; whereas billing changes cannot quickly adjust how customers user their broadband access (Cogeco 2009b), DPI enables a rapid modification of habit. Habits must be changed so that all users can enjoy their broadband access *and* let Cogeco mitigate congestion on their networks. In a similar vein, Rogers admits that large numbers of cable modems share the same download and upload ports (275 per downstream port and 100 per upstream port),

[6] While only Bell appears to have confirmed the use of DPI for subscriber management, we might infer that other Canadian ISPs are also doing so, on the basis that these appliances are commonly marketed to assist in managing subscriber connections.

and that P2P *uploads* must be managed to provide positive experiences for all users (Rogers 2009a).

With these uses in mind, let us return to the six-part list that was presented earlier and determine what appear to be the 'drivers' of DPI in Canada, and supplement our analysis with some of the critiques of network owners' use of DPI for traffic management purposes.

1. More precisely engage in lawful interception tasks/surveillance operations as mandated by police and intelligence communities.

While CALEA may motivate American ISPs to deploy DPI (Anderson 2007), and EU Directive 2006/24/EC (on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks) induce some European ISPs to justify the insertion of DPI appliances in networking infrastructures, it is unclear that a similar directive presently motivates Canadian ISPs.[7] While some ISPs have noted that DPI *could* be used to fulfill law enforcement demands, there are other networking processes that have always been able to capture traffic on behalf of authorities. Thus, law enforcement does not appear to be a central driver of DPI deployment in the Canadian situation.

2. Regulate content and enforce copyright.

In their public filings, Canadian ISPs regularly insist that the technologies that they are deploying cannot examine content that individuals transmit (Bell 2009a) or, alternately, are unwilling to examine content for legal reasons (Rogers 2009a and b; Cogeco 2009b; Bell 2009a). Moreover, to the accusation that the delaying of P2P content alone constitutes a regulation or control of content (as suggested by CDM, DOC, CBC-Radio Canada, IFTA), ISPs insist that the delay of content alone neither reshapes it meaning or influences its content. Further, while some DPI appliances claim to be able to regulate content insofar as they can prevent copywritten files from crossing a network (iPoque (2009) details these processes), no Canadian ISP has admitted to using equipment that can perform such actions. The Canadian copyright industry has been mute on the possibilities of these particular technologies, though it should be noted that in Ireland and Belgium European copyright groups have struggled (and thus far failed) to get DPI used to police copyright infringement (Bendrath 2009).

3. Manage bandwidth by limiting the use of 'problem' applications and more precisely manage subscriber access to services and bandwidth.

[7] At the same time, there have been several attempts to institute 'lawful access' legislation in Canada, which would require ISPs to capture data at the behest of authorities. The possibility of such regulation may be seen as driver for instituting DPI, but for the purposes of this paper I do not take up this potential driver.

The management of particular applications is a predominant concern – P2P is a 'problem', and discriminating against its traffic is a "good" form of discrimination because doing so "enhances the performance or efficiency of a network" (Telus 2009). This facilitates a more equal share of bandwidth being distributed amongst members of the network. In addition, Bell admits that their "DPI equipment was originally intended to introduce usage data collection functionality for Bell Wireline's usage billing" and was *subsequently* "used for traffic shaping as a necessary measure to address congestion at peak periods" (Bell 2009b). Bell's use of DPI crept beyond its original purpose to manage subscriber data but, even in its initial deployment, efficiency for customer service drove this technology's installation.

4. Enhance network security by using heuristics to watch for aggressive/harmful network activity.

While only Sasktel notes that they exclusively use DPI technologies for network security (Saskatchewan Telecommunications 2009; 8a), some advocate groups admit that there are situations where using DPI is appropriate (e.g. CDM 2009b) to limit dangers to the network itself. Thus, viral outbreaks are something that might be understood as "good" to discriminate against. At the same time, where 'aggressive or harmful' network activity is understood as P2P applications consuming a large allotment of bandwidth for prolonged periods that are generating congestion on ISPs' networks, network owners argue that this is an appropriate time to deploy DPI. In the CRTC proceeding on traffic management practices, this is a contentious issue where ISPs maintain that throttling P2P is appropriate, and many other parties suggesting otherwise, but regardless of the dispute it is clear that at least the network owners who lease their facilities and the advocates who worry about this technology concede the some forms of network security/management justify the limited uses of DPI equipment. The debate, in essence, surround questions of what kinds of activity merit "good" discrimination, what which efforts constitute "bad" (or perhaps "less bad") discrimination.

5. Facilitate vertical integration by discriminating against particular services in favor of others.

Canadian ISPs steadfastly insist that vertical integration of services, either through establishing 'walled gardens' or limiting competing services from intruding up the revenue structures of traditional content delivery mechanisms, does not drive the integration of DPI appliances into telecommunications networks. Perhaps the most forceful rejection of the claim that vertical integrate drives the insertion of DPI into Canadian networks comes from Shaw, when they write,

> The argument with respect to the alleged relationship between DPI traffic shaping and Shaw's own video services are equally baseless and without merit. First, there is absolutely no evidence to suggest that use of DPI traffic shaping has any impact whatsoever on the demand for Shaw's cable service, or that peer-to-peer sharing is even a substitute for cable service (Shaw 2009).

Rogers Communications maintains that it does not use DPI to establish walled gardens in mobile web environments, on grounds that it does not block wireless content, webpage "tracking codes", or webpages. At the same time, however, we might question how they define a walled garden, given that they admit they have

> . . . entered into commercial arrangements that allow our customers to browse the websites of our partners for free, obtain free content, or pay a package price including both. In many of these instances it is the partner who bears the cost of this traffic. In many cases, these arrangements include time limited promotions designed to generate interest, providing products and services to expose customers to new capabilities and hopefully encourage them to try new services (Rogers, 2009b).

While we could argue that in establishing preferential locations for mobile users to visit, Rogers is establishing a walled garden of sorts, we might be charitable and say that such a commercial aim isn't the goal of their *DPI appliances*, but instead emerges from other business arenas/relies on non-DPI technologies. The reason for this charity is that Rogers is not transparent about how they develop this garden-like environment, or how they monitor and direct data traffic amongst favored partners; we cannot be certain it is with the assistance of DPI devices, though it very well could be.

6. Use behavioural advertising to monetize citizens' web browsing and application-use habits

No Canadian ISP has admitted to using DPI for behavioural advertising purposes, which typically entails an ISP collecting data about users' web browsing history and then inserting advertisements on subsequent web pages that they visit based on expected shopping preferences. MTS Allstream insists that such forced ad injections would need to be supported by opt-in decisions; any other approach to such advertising would be inappropriate or wrong (2009).

Thus, on this basis there are at least no implicit reasons in the CRTC filings to suspect that a drive to monetize citizens' online habits motivates the deployment of DPI equipment based on what Canadian ISPs have submitted to the public record. This position ignore the discussions that telecom giants themselves are involved in, of course – the discourse of the 2009 Canadian Telecommunication Summit's persistent focus on DPI, data mining, tracking customer behaviour suggests that even if advertising is not a foregrounded force driving DPI deployment, it is not far from the mind of ISPs' marketing departments.

At the same time, we must admit that without a public notice *explicitly* focused on advertising practices that ISPs would have little/no reason to openly disclose their advertising expectations with these technologies in a proceeding on traffic management. Thus, we need to keep in mind that PN 2008-19 only provides limited insight into ISP aspirations – other sources can profitably be integrated into an analysis of ISP practices to develop a more holistic understanding of their business intents and practices concerning DPI. Still, having briefly discussed what might be driving the deployment of DPI technologies in Canada from the perspective of statements on the record concerning DPI itself, let us turn to how these technologies are *currently* being deployed to reinforce netscapes of power.

III – Techniques of obfuscation, avoidance, and refutation

Netscapes of power are intended to "buttress market power and to regulate behaviour through network architecture, the privatization of cyberlaw, surveillance, and the creation of walled gardens" (Winseck 2003). This can entail a set of divergent market and technological practices, but for our purposes we will focus on network architecture, the creation of walled gardens, and add a new category to Winseck's definition: the privatization of knowledge about network architecture itself. After outlining what constitutes these categories, I discuss how Canadian ISPs sabotage public insight into how DPI technologies are deployed in Canada. As a result, interested parties' abilities to penetrate the technical shells of these netscapes are curtailed. On the basis of these obfuscatory practices, I will conclude by arguing that privacy advocates would be well advised to adhere towards a fundamentalist, over a pragmatic, approach to privacy.

Network Architecture and Walled Gardens

In designing DPI into network topologies, ISPs are actively attempting to regulate what is used to transfer data across their networks. Presently, they are arguing before the public that impacting P2P data flows is a necessary facet of good network management – despite P2P's efficiency in distributing file transfers, it is inefficient insofar as it ignore the realities of the ISPs' underlying hardware infrastructures. Cable and ADSL providers operate asynchronous consumer networks, where more bandwidth is allocated for burst downloads/downstream access than for persistent uploading of data packets.

In Telus' case, even though they are not currently using DPI appliances to manage their network traffic, they want to make a distinction between "good" and "bad" packet discrimination. "Good discrimination enhances the performance or efficiency of a network, while bad discrimination harms the interests of users or other persons" (Telus 2009). In an attempt to avoid criticism of how DPI appliances delay the transfer of P2P packets, Shaw writes that because they only shaping upstream P2P traffic, and are not limiting individuals from downloading content, they are not attempting to regulate behaviour by directing consumers to non-P2P (e.g. traditional cable broadcast) content repositories (Shaw 2009). Similar assertions come from Rogers, who have gone so far as to note that not even P2P users complain about Rogers' practice of shaping traffic (Rogers 2009b).

While ISPs are justifying the potential to use DPI for traffic shaping purposes, and defending their use the technology is already installed and running, were DPI and its uses uncontroversial the CRTC would not be holding a proceeding surrounding the technology's bandwidth management applications. Consumer and media groups have stepped forward and insisted that ISPs are, in effect, working to regulate the actual content that flows through network. This argument tends to assert that regulation of P2P packet flows establishes an anti-competitive environment, where ISPs' own services are given precedence over emerging content delivery systems. The CBC insists that the very shaping of traffic content (which includes content that the CBC has distributed using P2P technologies) violates the Telecommunications Act because communication is significantly distorted simply by frustrating timely access to content (CBC 2009). The Independent Film & Television Alliance (2009) and the Canadian Film and Television Production Association (2009) share similar positions. In essence, all three argue that asymmetries of content distribution, and thus influence over the content that Canadians will engage with, are affected by modifying how quickly they can access that content. The Canadian Film and Television Production Association goes so far as to note that, "no Canadian broadcaster that is affiliated with an ISP or are part of a large corporate group has filed a submission in this proceeding. *Only independent broadcasters have participated in this proceeding, with all of them raising concerns about the risks associated with application- or protocol-specific traffic management practices*" (2009; emphasis added). In effect, the CFTA is concerned that the dominant carriers are establishing that netscapes that are facilitated by the discriminatory bandwidth management practices directed towards P2P network traffic.

We may be inclined to agree with these groups, and I argue that the discriminatory throttling of traffic does seem to be establishing a *contemporary* netscape; while content is not necessarily being *banned*, it is *more challenging to access* than alternate forms of media offered by major content distributors (who are often associated with ISPs in Canada). This contemporary netscape can be distinguished from prior iterations (e.g. AOL), insofar as individuals are *able to* access content from beyond the ISP's partners, but their range of choice are moderated by the throttling of particular content. Whereas prior netscapes were distinguished by constraining individuals by establishing web portals, current netscapes extend the allure of ISP portals by limiting over-the-top applications' technical capacities – why download something from the CBC at a throttled pace, when you could use an 'on demand' service provided by one of the major ISPs to immediately access content that is neither throttled nor contributes to your bandwidth restrictions?

What makes the contemporary netscape so potent is that in most cases all of the incumbent's customers, as well as wholesale customers, are affected by DPI-powered throttling. As a result, not only is the Bell netscape appealing for Bell users when it comes to video content, but it also becomes a point of competition that Bell can use to lure customers from competing downstream ISPs. Absolute control of the network means that wholesale ISPs are forced to compete at the level of service they can render to customers alone – they cannot compete at a 'technically-enhanced' level.[8] Thus, we would agree with Winseck when he writes that those who control

[8] While beyond the scope of this paper, it is important to note that smaller ISPs are also challenged to compete with Bell and other incumbents in terms of pricing; where an incumbent can unexpectedly increase rental fees to access a local loop, it is possible to force a smaller company out of business by

networks, “can exercise a great deal of influence over content providers’ access to users, and users’ access to content” (2003: 181). In the contemporary netscape ISPs can establish preferred content sources and types of content that is based on the ease and speed of access to material.

Primus directly addressed the concerns that netscapes are being established in their April 30th submission to the CRTC, writing:

> this issue [of asymmetrical competition] is exasperated by the fact that upstream ISPs have the ability to waive or exempt their end-users from traffic management practices, if they so choose. In Primus’ view, the ability of upstream ISPs to exempt their end-users from traffic management practices, such as usage-based billing, for winback or incentive purposes, while at the same time enforcing the same traffic management practices and policies on downstream ISP competitors that enjoy no such flexibility or recourse affords significant undue preference to the upstream ISP (2009).

Whereas downstream ISPs are tightly regulated by DPI rule sets, in the sense that their customers’ packets are surveyed and slowed depending on their content, and insofar as finite amounts of bandwidth are purchased without any ‘freebies’, dominant carriers are situated to waive rules when economic motivations are before them. This particular asymmetry is accented when dominant carriers, such as Shaw, Cogeco, and Bell, provide economic spaces where their customers can purchase the same video (or even alternate video) that is available through a P2P connection. The dominant carriers do not incur bandwidth-related charges when they allocate bandwidth so that their customer’s can access on the carrier’s on-demand content library, but this is not the case for either wholesaler ISPs or small groups who rely on P2P to release their content. These groups are financially unable to establish a competing infrastructure, and thus have no easy way of providing on-demand video services without incurring significant charges. Downstream ISP customers consequently are more reliant on P2P services, and video-on-demand services constitute a competitive advantage for dominant carriers.

The infrastructure that transmits content is not just subject to DPI-facilitated rule sets; in addition, the infrastructure itself is shrouded in relative secrecy. While various corporate agents in Canada have disclosed the broad specifications of how their networks operate (e.g. informing the public of the relationship between authentication points and local offices), they refuse to disclose the particular DPI appliances that reside within their network topologies.[9] The Public Interest

raising rates to the extent where they *lose* money on each customer. The downstream ISP is in a contractual agreement that limits their ability to rapidly change pricing structures, and Bell can force new practices on those customers without ever having signed a contract with them. Thanks to Priyantha Kumara for this insight.

[9] I have summarized all of the CRTC filings concerning network infrastructure at the following link. You will note that only Shaw and MTS Allstream disclosed the vendor that they worked with, but filed the actual appliances in confidence with the CRTC. Link: http://www.christopher-

Advocacy Center, in particular, was insistent that meaningful public participation in the CRTC proceeding would require the public knowing what DPI equipment was being used by ISPs; the breadth of devices and their varying capacities meant that honed comments required transparent disclosure of the networking appliances. Without this information, interested parties would be limited in their ability to accurately identify particular concerns with networking appliances and would instead be forced to speak vaguely in terms of what DPI appliances potentially could be used for (PIAC 2009).

In the face of these requests for disclosure, no ISP actually provided the equipment or model numbers of their appliances. Many were forced to reveal that they were, in fact, using DPI appliances by the CRTC (this information was initially filed in confidence by most carriers in the proceeding), but none were required to disclose the technical capacities of these devices to the public. The dominant carriers are unanimous that their technologies, as presently configured, do not allow for genuinely massive surveillance, with only CRTC officials knowing the veracity of these claims.

Cogeco has noted, in response to privacy and surveillance concerns raised by members of the public and advocacy groups that, "with respect to the possibility that DPI technology can look into the content of a message sent over the internet, like reading the content of an envelope sent by surface mail, Cogeco would like to make clear on the record of this proceeding that the DPI equipment implemented by Cogeco has limited capacity and is not used in any manner to identify the content embedded in the packets exchanged by P2P users on Cogeco's network. While, like any network device, these devices could allow examination of the content of a packet, it is simply not within the capability or capacity of these devices to so across the thousands of subscribers and multi gigabytes of traffic that traverse these devices per second (Cogeco 2009b). Note that, despite 'clarifying' the record, the public is left with no clearer understanding of what is being done to their packets now than they were prior to the proceeding. Are dominant carriers using DPI appliances that *can* be configured to respond to copyright infringement? Are the DPI appliances dominantly engaging in heuristic analysis of packet transfers, or are they examining the application layer? Do these devices permit the analysis of packets as they cross a router and, as flows are identified that correspond with input signature types, copy particular streams of data for offline analysis and release to authorities? In a limited fashion, can these devices be used for lawful intercept purposes?

Some DPI devices are touted as being able to perform all of these actions, but many cannot. Without disclosing information on their actual network topologies, consumer groups and interested Canadians are left guessing about what ISPs are using to monitor and adjust packet flows. Without an understanding of the technologies, ISPs can say that their devices are neither privacy invasive nor particularly useful for law enforcement without having to substantiate their

parsons.com/blog/isps/update-crtc-pn-2008-19-isp-filing-summary-document/

arguments before the public eye. By filing the equipment that is used to manage networks in confidence with the CRTC, ISPs effectively undermine the public's ability to critically engage with the capacities of these devices in a meaningful way.

Private Knowledge

Dominant carriers regularly remind members of the public that the CRTC is to focus exclusively on traffic management, and that DPI technologies are just an element of that broader effort of management. As a result, they insist that the proceeding cannot be about the technology itself;[10] to address the technology misses the point – what needs attending to are its particular uses. Only when a worrisome use is realized should the CRTC or other appropriate government agency get involved. Each dominant carrier has asserted that a case-by-case approach to the technology needs to be adopted, where particular applications of DPI and particular instances of traffic management are examined, rather broad rulings about the technology as a whole.

The problem for consumers is that it can be incredibly difficult to learn how DPI appliances are actually being used by carriers; in the United States it was largely by happenstance that ad injections (Topolski 2008) or Comcast throttling (Bangeman 2007) was identified as an instance of DPI use. Phorm recognizes that they need to achieve greater 'transparency', but rather than suggesting that this means a greater degree of public divestiture of their operations, it means that end-users should never realize that Phorm is combing their traffic to insert advertising (BT Retail Technology 2007). Achieving 'transparency' when using DPI appliances means that individuals cannot determine the source of delayed packet transmissions or modified web pages; is it a bad application, a bad file transfer, or (in the case of a wholesale ISP customer) interference from my ISP's ISP?

Refusing to disclose the discriminatory elements of the common carriage system thus creates the netscape. Avoiding or limiting this netscape doesn't *necessarily* require dominant carriers to reveal the particular devices installed on their network, but at least requires them to provide complete and honest accounts of the devices' full range(s) of possibilities and capacities. Without detailed accounts of what is possible with these technologies – instead of merely stating that they are 'not privacy invasive' – advocates cannot develop concrete arguments based on the particular merits and disadvantages of the DPI appliances that are in use. This establishes an epistemic distance between ISPs and interested parties; parties are forced to 'trust' ISPs. As has been noted by new competitors in the wireless data and voice market, consumers have long memories when it comes to telecommunications companies, and they have developed a significant distrust of the longstanding dominant carriers (Canadian Telecom Summit 2009).

[10] At the Computers, Freedom, and Privacy 2009 panel on Deep Packet Inspection, it is noteworthy that almost all of the participants recognized that DPI does have some valid uses, such as assuring network security. This included consumer groups and researchers who have been critical of the use of DPI.

In light of the development of network topologies that are shrouded in mystery, along with the development of contemporary walled gardens and epistemic privileges, consumer and privacy advocates would be well advised to adopt a more 'fundamentalist' stance towards consumer and privacy protection. In the following section I briefly outline the fundamentalist and pragmatic privacy positions, and why a more fundamentalist stance is appropriate for the current Canadian situation.

IV – The Fundamentalist Approach

In his recent research into the nature of privacy advocates around the world, Colin Bennett developed a six-part typology of advocates. It is his first category, that of privacy activists, that I want to first address and describe how these activists relate to what I am terming 'privacy fundamentalists'. I will follow by briefly offering an account of a privacy pragmatist, and conclude by arguing that the evidence of function creep, combined with dominant carriers' market power and epistemic privileges, mean that advocates ought to lean towards fundamentalist, rather than pragmatic, stances when engaging Canadian ISPs on issues pertaining to DPI technologies.

The Activist/Fundamentalist

Activists are differentiated from advocates, insofar as they are 'seen to be doing something'. These individuals and groups "do not balance privacy against competing public interests, because they know that the opposing arguments will always be made with force and by people with far more resources than they have. For some advocates, the privacy argument requires uncompromising articulation rather than negotiation with competing social interests" (Bennett 2009). Principles fuel activists, and they are not interested in 'balancing' their principles with other social interests or technological aims. The ideal type of activist is solely devoted to the 'cause' of privacy (however that happens to be defined), and is rarely forced to compromise their principles for financial or political reasons.

In adopting deep seated, ideally unshakeable principles, activists are often drive by what Daniel Solove terms 'nonconsequentialist accounts of privacy's value.' These accounts can be grounded in a Kantian or neo-Kantian rights-based discourse, where freedom and autonomy of persons are seen as a core, or even necessary, social good (Solove 2009). Securing the individual's, and society's, privacy rights is necessary to guarantee the dignity of each member of society; even when information is gleaned about a person without intent to generate harm or influence their behaviour that inspection must be resisted.

With entrenched attitudes concerning privacy that are (hopefully) grounded in argumentative reason and fact, fundamentalists will oppose new technologies that they perceive entering a market and endangering whatever conception of 'privacy' they happen to hold. Such definitions are not necessarily identical, or based on the same foundations; privacy advocates of various stripes, motivations, economic and social backgrounds are well known to band together when a common threat faces them (Bennett 2009). These groups are not necessarily concerned with the intricacies of a problem – what DPI might solve, what it might be possible or incapable of doing – and instead argue on the basis of principle. While principle guides the privacy pragmatist as well, they tend to adopt more flexible approaches to privacy concerns.

The Pragmatist

Pragmatists perceive a need to modulate radical or extreme privacy positions if they are to have a seat at the bargaining table that is deciding how to implement a privacy compromising action or policy.[11] Simon Davies terms these individuals 'pragvocates' (Bennett 2009). Daniel Solove writes that these individuals acknowledge that "[p]rivacy should be weighed against contrasting values, and it should win when it produces the best outcome for society. A pragmatic approach to valuing privacy involves balancing it against opposing interests . . . We determine the value of privacy when we seek to reconcile privacy with opposing interests in particular situations" (Solove 2008: 87). Whereas privacy fundamentalists will uphold particular understandings of privacy regardless of the social situation, pragvocates wants to know what the situation on the ground is; what technology is being deployed, how might privacy be compromised, are there methods of ensuring that privacy interests are upheld while meeting the compromiser's goals?

This stance is sometimes evidenced in the actions of Canada's privacy commissioners; they often work *with* companies, rather than operating as fundamentalist advocates of privacy. Such actions reveal beliefs that cooperation leads to more deeply engrained privacy protection in most cases than adversarial engagements. Pragmatists, such as Dr. Ann Cavoukian, insist that it is important to work within an existing system and adjust it so that all parties win (Brown 2009). This attitude orients her 'PET+' and 'Radical Pragmatism' approaches to guaranteeing privacy in a digital world; by integrating privacy enhancing technologies into the very infrastructure and code of otherwise privacy compromising activities, it is possible to meet social interests aimed at maintaining personal privacy while also meeting corporate and governmental surveillance objectives (Cavoukian 2008).[12]

It would be wrong to assume that pragmatists are somehow themselves 'compromised' or have 'turned coat'. Adopting case-by-case approaches, where they rigorously consider the facts of a situation and then make recommendations based on the facts of the environment, is a challenging and oftentimes socially rewarding

[11] I adopt the term 'privacy compromising' to reflect the notion that individuals or societies are manoeuvred to offer up facets of information/allow for (re)combinations of information that can be used to discriminate between the delivery of goods, services, and so forth to particular individuals and groups. This diverges from 'invading' privacy, insofar as compromise assumes some process of negotiation, though at differing degrees of legitimacy and explicitness.

[12] One can certainly see how the PET+ agenda integrates with Lawrence Lessig's (2006) account of code, where only by integrating democratically legitimated principles within the core infrastructure of technology can democratic and constitutional values be maintained in our techno-code driven societies.

task. Their actions are often rooted in empirical fact and grounded in a principle of fairness that encompasses groups that may be compromising privacy as well as those who are being compromised. This pragmatic sensibility, combined with empirical evidence, enables pragvocates to extend their influence to governmental decisions, where providing useful information to regulators leads to heightened personal and organizational respectability (Bennett and Raab 2006). Such respectability can be leveraged in subsequent privacy-related drives, meaning that 'successful' pragvocates are far more likely to have a hand in steering how privacy compromising policies are developed than fundamentalists, who often stand outside the corridors of power.

Canadian Privacy Advocacy and DPI

What I see as key to these discussions, however, is that the pragmatist often depends more highly on empirical information to engage in a case-by-case approach to potential compromising actions than the activist. While activists are certainly not *opposed* to learning about the situation, they are more willing to modulate information for their own fundamentalist purposes.[13] The challenge before privacy (and, by extension, consumer) advocates is that it is difficult to engage in an empirical approach to DPI devices deployed by Canadian ISPs on a case-by-case basis because of the phenomenal lack of empirical data that has been made available to the public. As a result, while a pragmatic approach is needed to *temper* an activist position, we must worry about the potentialities of DPI devices as they relate to the possibility of massively compromising Canadians' privacy. The danger in focusing on a case-by-case approach, without knowledge of what the devices can natively be configured to do, is that while *at the moment* they may not be configured to massively compromise Canadians' privacy, a reconfiguration might go unnoticed because of the secrecy cloaking ISPs' networking operations. While at the moment the devices are presumably configured for the purposes of economic efficiencies, will they remain so configured in perpetuity?

It is this lingering question and accompanying worries that haunts the activist, and what motivates opposition to these technologies. While pragvocates may work within the system, taking account of the broader variables that likely direct ISPs in their present attitudes with these devices, they would be well served to ask what is next, and what is possible. I would suggest that a full-blown fundamentalist position is unlikely to be helpful in engaging in discussions of DPI appliances in Canada, but that a strident voice the opposes the compromising of privacy ought to be adopted given the relative lack of information that ISPs have places on the public record about the potential of their devices. Given that we have already seen Bell take advantage of their devices' potentialities when they expanded their use from subscriber monitoring to P2P traffic throttling, we would be well served to keep in mind other possible avenues of function creep. Adopting a dominantly case-by-case analysis of technologies without knowing their specific attributes risks missing the

[13] Groups such as CASPIAN and Bad Phorm arguably fit within this typography.

concerns and dangers related to DPI-enabled function creep; it risks missing the forest through the trees.

Conclusion

Contemporary netscapes of power are distinct from the early walled gardens of AOL, and are being facilitated by the insertion of DPI networking appliances into Canadian ISPs' infrastructures. These netscapes have consequences for content producers as well as privacy advocates who worry about the latent capacities of these appliances. While economic and efficiency motivations have propelled the purchase and configuration of these appliances to date, in the face of lawful access legislation, discourse surrounding the monetization of consumer data traffic, and rhetoric of DPI manufacturers themselves Canadians would be well served to be skeptical of the full, versus presently realized, potentials of these appliances. Emergent with this skepticism, I have argued that a simple case-by-case approach to DPI in Canada risks missing the forest through the trees – while there is certainly a case to be made for a dominantly pragmatic approach to engaging with these technologies, the fact function creep has already occurred combined with ISPs' unwillingness to publicly disclose their devices' technical capacities warrants adopting a more fundamentalist than pragmatic approach. Questions about the technology itself must be asked. Do we want a messier/less functional network environment? Do Canadians want regulation that stunts these devices' surveillance possibilities, at the expense of efficiency gains/higher monthly bills? Should DPI be used to discriminate between packets and packet streams, or should another technology (perhaps more expensive to deploy/less effective) be used instead?

While developing regulations to respond to these questions might be perceived as heavy handed, a heavy-handed response is often the consequence of substantial public ignorance about an issue. Canadian ISPs have facilitated and promoted this ignorance by refusing to publicly disclose the full range of capabilities of their devices to the public – in the face of such intentionally promoted ignorance, the public can hardly be faulted for defaulting to a more privacy fundamentalist position and demanding heavy-handed regulation. It will be up to ISPs to head off such legislation, hopefully through increased public transparency.

Works Cited

Allot Communications Ltd. (2007) "Digging Deeper into Deep Packet Inspection," Published 2007.

Anderson, Nate (2007). "Deep packet inspection meets 'Net neutrality, CALEA," *ArsTechnica*. Published July 25, 2007. Last accessed June 28, 2009. URL: http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars

Arbor Ellacoya (2008). *Arbor Ellacoya e100: Unmatched Scale and Intelligence in a Broadband Optimization Platform (Datasheet)*. Last accessed: December 23, 2008. URL: http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=355

Bangeman, Eric (2007). "Comcast shooting itself in the foot with traffic "explanations"," *ArsTechnica*. Published October 23, 2007. Last accessed June 28, 2009. URL: http://arstechnica.com/old/content/2007/10/comcast-shooting-itself-in-the-foot-with-traffic-shaping-explanations.ars

Bell Aliant/Bell Canada (Bell) (2009a). "Telecom Public Notice CRTC 2008-19, Review of Internet management practices of Internet providers (PN 2008-19) – Comments," filed to CRTC February 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029804.zip

Bell Aliant/Bell Canada (Bell) (2009b). "Telecom Public Notice CRTC 2008-19, Review of Internet management practices of Internet providers (PN 2008-19)," filed to CRTC January 13, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1006810.zip

Bendrath, Ralf (2009). "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection (first draft)," prepared for International Studies Annual Convention. New York city, February 15-18 2009. Last accessed June 28, 2009. URL: http://userpage.fu-berlin.de/%7Ebendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf

Bennett, Colin (2009). *The Privacy Advocates*. Cambridge, Massachusetts: The MIT Press.

Bennett, Colin and Charles Raab (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, Massachusetts: The MIT Press.

Bivio Networks and Solera Networks (2008). *White Paper: Complete Network Visibility through Deep Packet Inspection and Deep Packet Capture*. Lindon, Utah: Solera Networks. Last accessed December 25, 2008. URL: www.soleranetworks.com/products/documents/dpi_dpc_bivio_solera.pdf

Brown, Jesse (2009). "CCTVs, Biometrics, and self-destructing data," *CBC Podcast*. Published March 15, 2009.

BT Retail Technology (2007). "PageSense External Technical Validation", dated Jan 15, 2007. Last accessed June 28, 2009. URL: https://secure.wikileaks.org/wiki/Image:BT_Report.pdf

Cavoukian, Ann (2008). *Privacy and Radical Pragmatism: Change the Paradigm*. Ontario: Government of Ontario.

Campaign for Democratic Media (CDM) (2009a). "Telecom Public Notice CRTC PN 2008-19: Review of the Internet Traffic Management Practices of Internet Service Providers," filed to the CRTC April 30, 2009.

Campaign for Democratic Media (CDM) (2009b). "Telecom Public Notice CRTC 2008-19, Review of Internet management practices of Internet providers

Comments of the Campaign for Democratic Media," filed to the CRTC February 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029987.zip

Canadian Broadcasting Corporation (CBC) (2009). "Review of the Internet traffic management practices of Internet service providers, Telecom Public Notice CRTC 2008-19, 20 November 2008 - Initial Comments of CBC/Radio-Canada," filed to CRTC February 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030285.PDF

Canadian Film and Television Production Association (CFTPA) (2009). "Reply Comments to the Canadian Film and Television Production Association With respect to: Telecom Public Notice CRTC 2008-19: Review of the Internet traffic management practices of Internet service providers," filed to the CRTC April 30, 2009. Last accessed June 28, 2008. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1111275.pdf

Canadian Telecom Summit (2009). Advanced Wireless Services – The new kids on the block panel. Toronto, June 15-17, 2009.

Cogeco (2009a). "Telecom Public Notice CRTC PN 2008-19, Review of the Internet traffic management practices of Internet service providers – Cogeco Submission," filed to the CRTC February 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/102968

2.pdf

Cogeco (2009b). “CRTC File No: 8646-C12-200815400 - Telecom Public Notice CRTC 2008-19, Review of the Internet traffic management practices of Internet service providers - Cogeco Reply Comments,” filed to CRTC April 30, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1110488.pdf

Documentary Organization of Canada (DOC) (2009). “Telecom Notice of Public Consultation and Hearing CRTC 2008-19 Call for Comments on Internet traffic management practices of Internet service providers,” filed to the CRTC February 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030141.PDF

Independent Film and Television Alliance (IFTA) (2009). “Public Notice 2008-19 – Review of the Internet traffic management practices of Internet service providers. Reference No. 8646-C12-200815400,” filed to CRTC February 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1032007.DOC

Internet Innovation Alliance (IAA) (2007). “What is the Exaflood?” video presentation on YouTube. Last accessed June 28, 2009. URL: http://www.youtube.com/watch%3Fv%3DwVnH5D-lWrA%26feature%3Dplayer_embedded

ipoque GmbH (2008a). *PRX Traffic Manager (Datasheet)*. Leipzig: ipoque GmbH. Last accessed December 24, 2008. URL: www.ipoque.com/userfiles/file/datasheet-prx1000-prx2000-prx5g-rev2008-09-23-web.pdf

ipoque GmbH (2009a). *Internet Study 2008/2009*. Leipzig: ipoque GmbH. Last accessed June 28, 2009. URL: http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009

ipoque GmbH (2009b). *Copyright Protection on the Internet*. Leipzig: ipoque GmbH. Last accessed June 29, 2009. Accessible via: http://www.ipoque.com/resources/white-papers

Melcalfe, Bob (1996). “Yes! The Internet is on the verge of collapse” at Network World website. Last accessed June 28, 2009. URL: http://www.networkworld.com/netresources/1118metcalfe.html

MTS Allstream (2009). “Telecom Public Notice 2008-19, Review of the Internet traffic management practices of Internet service providers – Reply Comments,” filed to CRTC April 30, 2009. Last accessed June 28, 2009. URL:

http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1109931.pdf

Nowack, Peter (2008). "Canada's broadband networks not ready for future: report" at CBC website. Last accessed June 28, 2009. URL: http://www.cbc.ca/technology/story/2008/09/15/tech-broadband.html

Phorm (2009). "Advertisers and Phrom," Phrom corporate website. Last accessed June 28, 2009. URL: http://advertising.phorm.com/advertisers.php

Porter, Thomas, Andy Zmolek, Jan Kanclirz, and Antonio Rosela (2006). *Practical VoIP Security: your hands-on guide to Voice over IP (VoIP) security*. Rockland, Mass.: Syngress Publishing, Inc.

Primus (2009). "Review of the Internet traffic management practices of Internet service providers, Telecom Public Notice CRTC 2008-19 – Reply Comments," filed to the CRTC April 30, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1110635.pdf

Public Interest Advocacy Centre (PIAC) (2009). "Requests for Public Disclosure of Information Filed in Confidence with the Commission (Rogers)," filed to CRTC January 19, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1009391.zip

Rogers (2009a). "Telecom Public Notice CRTC 2008-19: Review of the Internet traffic management practices of Internet service providers," filed to CRTC Feb 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029665.zip

Rogers (2009b). "Telecom Public Notice CRTC 2008-19 – Review of Internet traffic management practices of Internet service provider – Rogers Reply Comments," filed to CRTC April 30, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1110392.pdf

Saskatchewan Telecommunications (SaskTel) (2009). "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers," filed to CRTC January 13, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1006369.zip

Shaw (2009). "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers – Reply Comments," filed to CRTC April 30, 2009. Last accessed June 28, 2009. URL:

http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1109885.pdf

Shaw, Gillian (2008). "Canadians spend close to a third of their leisure time online" at Vancouver Sun website. Last accessed June 28, 2009. URL: http://communities.canada.com/vancouversun/print.aspx?postid=255831

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

Swanson, Bret (2007). "The Coming Exaflood" at Wall Street Journal website. Last accessed June 28, 2009. URL: http://online.wsj.com/article/SB116925820512582318.html

Telus (2009). "Telecom Public Notice CRTC 2008-19, Review of the Internet traffic management practices of Internet service providers (20 November 2008) – Comments," filed to CRTC February 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029656.pdf

Tobkin, Chris, and Daniel Kligerman (2004). *Check Point Next Generation with Application Intelligence Security Administration*. Rockland, Mass.: Syngress Publishing, Inc.

Topolski, Robert M. (2008). "NebuAd and Partner ISPs: Wiretapping, Forgery, and Browser Hijacking," Free Press and Public Knowledge.

Unions des Consommateurs (2009). "Observations: De l'Union des consommateurs dans l'avis public de telecom, CRTC 2008-19," filed to CRTC Feb 23, 2009. Last accessed June 28, 2009. URL: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029374.zip

Winseck, Dwayne (2005). "Netscapes of power: convergence, network design, walled gardens, and other strategies of control in the information age" in David Lyon (ed), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. New York: Routledge.