thenewtransparency
surveillance and social sorting

**Working Paper**

# Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials

by Christopher Parsons[*]

## Abstract

Internet Service Providers (ISPs) are responsible for transmitting and delivering their customers' data requests, ranging from requests for data from websites, to that from file-sharing applications, to that from participants in Voice over Internet Protocol (VoIP) chat sessions. Using contemporary packet inspection and capture technologies, ISPs can investigate and record the content of unencrypted digital communications data packets. This paper explains the structure of these packets, and then proceeds to describe the packet inspection technologies that monitor their movement and extract information from the packets as they flow across ISP networks. After discussing the potency of contemporary deep packet inspection devices, in relation to their earlier packet inspection predecessors, and their potential uses in improving network operators' network management systems, I argue that they should be identified as surveillance technologies that can potentially be incredibly invasive. Drawing on Canadian examples, I argue that Canadian ISPs are using DPI technologies to implicitly 'teach' their customers norms about what are 'inappropriate' data transfer programs, and the appropriate levels of ISP manipulation of customer data traffic.

Version 1.2 :: January 10, 2008.

[*] Doctoral student in the University of Victoria's Political Science department. Thanks to Colin Bennett, Andrew Clement, Fenwick Mckelvey and Joyce Parsons for comments.

# Introduction

Internet Service Providers (ISPs) are uniquely situated to monitor electronic data traffic because all traffic to and from the Internet must pass through their networks. Using contemporary packet inspection and capture technologies, ISPs can investigate and capture the content of unencrypted digital communications, such as MSN messages, e-mail, and cellular text messages. This paper traces the lineage of contemporary packet inspection technologies and begins to raise both possible, and currently realized, surveillance issues.

I begin by describing the seven-layer model that structures the data packets that flow across ISP networks. Next, I offer accounts of the Shallow, Medium, and Deep Packet Inspection technologies, describing their respective capacities and limitations. I then identify how DPI devices can help ISP network owners, and conclude by drawing on Canadian examples to argue that ISPs are using DPI technologies to implicitly 'teach' their customers norms about 'inappropriate' data transfer programs, and about the appropriate levels of ISP manipulation of customer data traffic.

# 1 - The Origin and Constitution of the Packet

Email is one of the most widely used online services. When its transmission standard was codified in 1979,[1] it quickly became ARPANet's 'killer app' (Gudea 2004). Whereas communications were previously point-to-point (e.g. a letter or telegraph could be sent to one person at a time), email empowered individuals and groups to send a message to multitude of people simultaneously.[2] When an email message is sent, the content of the message is broken into a series of data packets. These packets can, at a general level, be understood as being composed of two parts: the header, and the payload or content.

The header information includes the recipient's Internet Protocol (IP) address, a number that is used to reassemble packets in the correct order when recompiling the messages, and is used to deliver the packet to its destination. Unlike in a circuit network, packets can travel to their destination using different routing paths. Header information is, in part, used to arrange packets in the correct order when they arrive at their destination. At a more granular level, the information used to route packets is derived from the physical, data link, network, and transport layers of the packet. The payload, or content, of the packet includes information about what application is sending the data, whether the packet's contents are themselves encrypted, and what the precise content of the packet is (e.g. the actual text of an email). More specifically, the payload can be understood as composing the session layer, presentation layer, and application layers of the packet.

These granular divisions of packets' header and payload are derived from the Open Systems Interconnect (OSI) model (Figure 1), which is composed of seven layers. This model was developed by the International Standards Organization (ISO) in 1984 to standardize how networking technologies were generally conceptualized. Over the course of this paper, I will refer to the OSI model when referring to the layers that packet inspection technologies can analyze, largely because packet inspection technology classes are often identified by their ability to examine data according to this model.[3] (For example, ipoque's PRX-1000, -2000, -1G, and -5G are all listed in their datasheets as identifying Layer-7 protocol activity, and Arbor/Ellacoya's e100 is noted for its ability to inspect data packets Layers 3-7.) Generally, the closer an inspection technology gets to surveying the application layer part of the payload, the more that the technology can learn about the packet passing through the inspection device.

[1] Email got off to a rocky start – when ARPANet was still the only major digital data network David Crocker, John Vittal, Kenneth Pogran, and Austin Henderson published *Request for Comments (RFC 733)*, to establish a uniform messaging standard in 1977. It wasn't, however, until Jon Postel summarized the *Computer Mail Services Meeting (RFC 808)* that an email standard was agreed upon.

[2] Radio and television allows for widespread, simultaneous, diffusion of content as well. These technologies, however, are regulated in a manner that limits the ability of individual members of the public to easily avail themselves of these transmission mediums.

[3] Appendix I has a visual mapping of major communication protocols (e.g. FTP, TCP, IP, IPX) in relation to the OSI model.

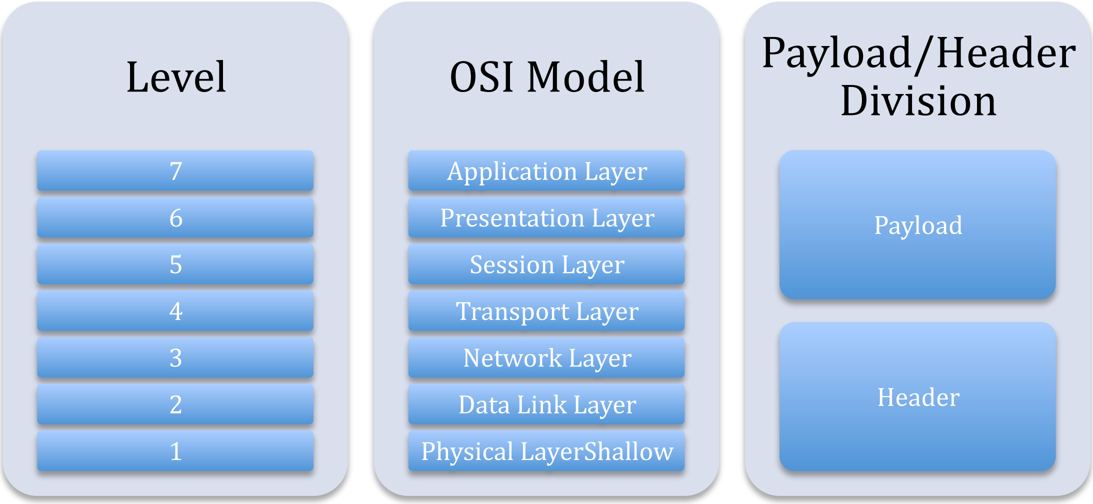


**Figure 1: Levels in OSI Packet Model**

When sending a packet of data, the *Application Layer* actually interacts with the piece of software that is making a data request (e.g. email client, web browser, instant messaging software, etc.). For example, when you enter a URL into a web browser, the browser makes a HTTP request to access a webpage, which is passed to the lower layers of the packet. When the browser receives a response from the server on the Internet that hosts the requested page, the browser displays the content associated with the URL. The *Presentation Layer* is concerned with the actual format that the data is presented in, such as the JPEG, MPEG, MOV, and HTML file-types. This layer also functions as the layer that encrypts and compresses data. In the case of a webpage, this stage is where the data request is identified as asking for a HTML file. The fifth layer, the *Session Layer*, creates, manages, and ends sessions' communications between the sender(s) and recipient(s) of data traffic – it effectively operates as a 'traffic cop' by directing data flows. When navigating to a URL, this layer regulates the transmission of data composing the web pages, the text, the images, the audio associated with it, and so on. These three layers broadly compose what is termed the 'payload' of a packet.

The fourth through first layers of a packet compose what is commonly referred to as the 'header'. The *Transport Layer* segments data from the upper levels, establishes a connection between the packet's point of origin and where it is to be received, and ensures that the packets are reassembled in the correct order. This layer is not concerned with managing or ending sessions, only with the actual process of connecting between the sender(s) and recipient(s) of packets. In terms of a web browser, this layer is intended to establish the connection between the computer requesting data, and the server that is hosting it, and with the proper ordering of packets of data that stream to and from the server. The *Network Layer* provides the packet's addressing and routing; it handles how the packet will get from one part of the network to another, and it is responsible for configuring the packet to an appropriate transmission standard (e.g. the Internet Protocol). This layer is not concerned with whether packets arrive at their destination error free – the transport layer assumes that role. The *Data Link Layer* formats the packet so that it can be sent along the mediums being used in transmitting the packet from its point of origin to its destination; this can mean that it is prepared for the wireless medium when sending an email from a local coffee shop, then re-packaged to be sent along an Ethernet connection as it travels to an ISP and through its networks and then back to a wireless format when being received by a colleague in their office who's laptop is connected to their local network using wireless technology. The *Physical Layer* doesn't change the packet's actual data; it defines the actual media and characteristics along which the data are being transmitted along.

Packets are transmitted from clients to servers. Figure two provides a visual presentation of a basic client-server transaction. These transactions begin with a client computer requesting data from a server by encoding a packet using the OSI layer model (i.e. creating a packet that contains the information from layers 7 to 1). The server receives the request, decodes it, and then encodes a packet response for the client, which subsequently

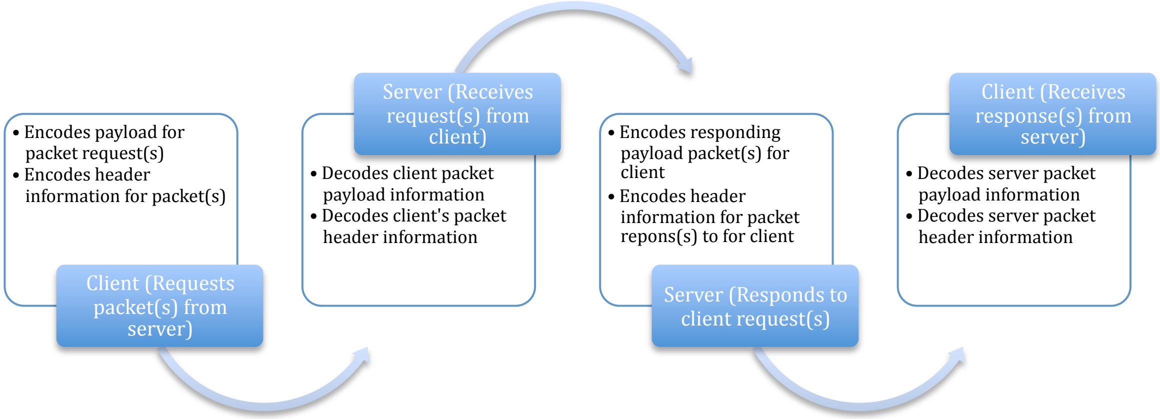

• Encodes payload for packet request(s)
• Encodes header information for packet(s)
Client (Requests packet(s) from server)
Server (Receives request(s) from client)
• Decodes client packet payload information
• Decodes client's packet header information
• Encodes responding payload packet(s) for client
• Encodes header information for packet repons(s) to for client
Server (Responds to client request(s)
Client (Receives response(s) from server)
• Decodes server packet payload information
• Decodes server packet header information

**Figure 2: Basic client-server transaction relationship**

receives and decodes the packet to provide the application with the requested information.

## 2 - Crossing the Packet Inspection Pool

Packet analysis technologies have been in use for over 15 years. In this section, I provide an explanation of three 'classes' of packet inspection technologies that have been, and continue to be, used in networking environments. When discussing the classes of 'shallow', 'medium', and 'deep' packet inspection, I refer to the OSI model to express the extent of information that these inspection technologies can derive from packets. Figure three provides a visual reference for the depth of inspection each of these technologies allows for. After discussing the capacities of these three packet inspection classes, I proceed to address the benefits of this mode of data inspection for network providers and why it is closely associated with contemporary data surveillance concerns.

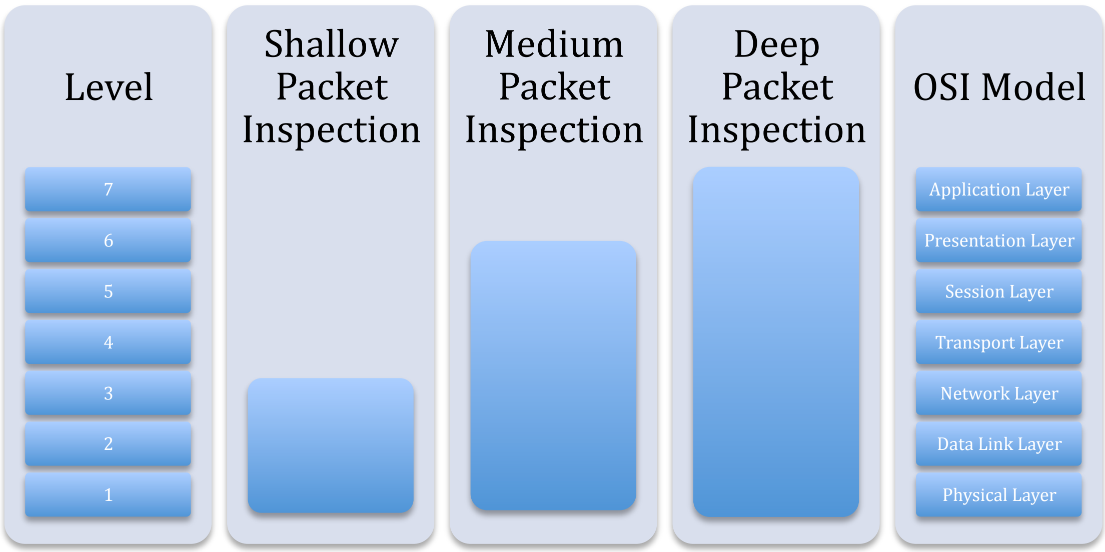


**Figure 3: Packet inspection depths**

## Shallow Packet Inspection

Shallow Packet Inspection (SPI) technologies drive the (relatively) simplistic firewalls found in the most recent generations of operating systems, such as Windows XP, Windows Vista, and OS X. These firewalls stand between a particular client computer and the network that it is attached to. They limit user-specified content from either leaving, or being received by, the client computer.

When a server sends a packet to a client computer, SPI technologies examine the packet's header information and evaluate it against a blacklist. In some cases these firewalls come with a predefined set of rules that constitute the blacklist that they evaluate data against, whereas in others network administrators are responsible for creating and updating the ruleset. Specifically, these firewalls focus on the source and destination IP address that the packet is trying to access. If the packet's header information is on the blacklist, the packet is not delivered. When SPI technology refuses to deliver a packet, the technology simply refuses to pass it along without notifying the source that the packet has been rejected.[4] More advanced forms of SPI capture logs of incoming and outgoing packet headers' source/destination information so that a systems administrator can later review the aggregate header information to adjust, or create, blacklist rulesets.

[4] The action of rejecting packets without notifying their source is sometimes referred to as 'blackholing' packets. It has the relative advantage of not alerting the sources that are sending viruses, spam messages, and so on that their packets are not reaching their destination.

SPI cannot read beyond the information contained in a header and focuses on the second and third layers in the OSI model; SPI examines the sender's and receiver's IP address, the number of packets that a message is broken into, the number of hops a packet can make before routers stop forwarding it, and the synchronization data that allows for reassembling the packets into a format that the receiving application can understand. This means that SPI *cannot* read the session, presentation, or applications layers of a packet; it is unable to peer inside a packet's payload to survey the packet's contents.

## Medium Packet Inspection

Medium Packet Inspection (MPI) is typically used to refer to 'application proxies', or devices that stand between end-users' computers and ISP/Internet gateways. These proxies can examine packet header information against their loaded parse-list.[5] Application proxies are typically placed inline with network routing equipment – all traffic that passes through the network must pass through the proxy device – to ensure that network administrators' rule sets are uniformly applied to all data streaming through the network. This has the benefit of separating the source and destination of a packet – the application proxy acts as an intermediary between client computers and the Internet more broadly – and enables network administrators to force client computers to authenticate to the proxy device before they can receive packets from beyond it. Figure three offers a visual example of how this might appear in a network.

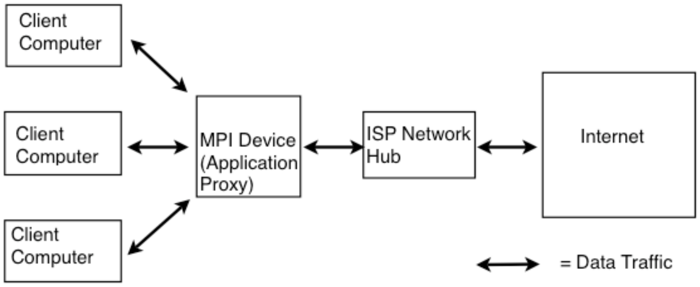


**Figure 4: MPI Device Inline with Network Routing Equipment**

When a packet enters the proxy, it is analyzed against a parse-list that systems administrators can easily update. A parse-list is somewhat more subtle than a blacklist. Whereas the latter establishes that something is either permissible or impermissible, a parse-list allows specific packet-types to be allowed or disallowed based on their data format types and associated location on the Internet, rather than on their IP address alone. Using MPI devices, administrators could prevent client computers from receiving flash files from YouTube, or image files from social networking sites. MPI technologies can prioritize some packets over others by examining the application commands that are

[5] It should be noted that, in addition to MPI being found in application proxies, some security vendors such as McAfee and Symantec include MPI technology in their 'prosumer' firewalls, letting their customers enjoy the benefits of MPI without paying for a dedicated hardware device.

located within the application layer[6] and the file formats in the presentation layer (Porter et. al. 2006). MPI devices suffer from poor scalability, insofar as each application command or protocol that is examined requires a unique application gateway, and inspecting each packet reduces the speed at which the packets can be delivered to their recipients (Tobkin and Kligerman 2004). Given these weaknesses, MPI devices are challenging to deploy in large networking operations where a large variety of applications must be monitored. This limits their usefulness for ISPs, where tens of thousands of applications can be transmitting packets at any given moment.

What is most significant, for our purposes, is that MPI devices can read the presentation layer of the packet's payload and identify facets of the application layer, making this technology important because it represents an important step towards the contemporary Deep Packet Inspection technology.

## Deep Packet Inspection

Deep Packet Inspection (DPI) technologies are customarily found in expensive routing devices that are installed in major networking hubs. These devices are intended to allow network operators precisely to identify the origin and content of each packet of data that passes through these hubs. Arbor/Ellacoya note that their e100 devices use, "DPI technology to monitor and classify data directly from your network traffic flow. Inspecting data packets at Layers 3-7 allows the e100 to provide crucial information to your operations and business support systems, without compromising other services" (Arbor/Ellacoya Networks 2008). Whereas MPI devices have very limited application awareness, DPI devices have the potential to "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). While MPI devices have issues with scaling to meet multiple applications protocols, DPI devices are designed to determine what programs generate packets, in real-time, for hundreds of thousands of transactions each second.  They are designed to scale in large networking environments.

In some cases DPI devices cannot immediately identify the application that has produced a packet. When this occurs, ISPs can use 'Deep Packet Capture' (DPC) technologies to collect packets in device memory and subsequently inspect them using DPI technologies. DPC lets network administrators perform forensic analysis of packets; packets that are captured are investigated using DPI to determine "the real causes of network problems, identify security threats, and ensure data communications and network usage complies with outlined policies" (Bivio Networks and Solera Networks 2008). Packets can be either fully captured, or only have particular characteristics (e.g. IP destination, port the packet used, application-type, etc) captured. After a DPC process, packet streams can be evaluated against sets of known applications and their corresponding data stream patterns using DPI so that ISPs can ensure that their security and data usage policies are being met

[6] Application commands are typically limited to Telnet, FTP, and HTTP.

by their customers; as an example, using this technology a new file sharing program's packet stream (which was unfamiliar to the DPI device) could be captured and subsequently analyzed and identified. Following this identification of this new program's packet stream, each packet from that program could have rulesets applied to it that corresponded with the ISP's networking policies.

To properly identify a packet, hundreds or thousands of packets can be stored in packet inspection device's memory until it has enough information to appropriately match the packets against the devices' list of known packet-types (Allot Communications Ltd. 2007). Once the device can match the previously ambiguous packets against its list of known packet contents, it knows what application (or application-type) is generating and sending the packet, and rules can be applied to allow or disallow the application(-type) from continuing to send and receive packets. Rules could, alternately, moderate the rates of data flowing to and from the application – this intentional alteration of data flow rates is often referred to as 'throttling'. While it is theoretically possible for all data to be captured using DPC technologies and subsequently analyzed using DPI appliances, this would substantially slow the transmission of packets and degrade user experiences of streaming content. DPC is not marketed to persistently capture all of the data that ISPs' customers send and receive; it's states uses is to for targeted capturing of packets to improve network subsequent network performance and to comply with regulatory demands (e.g. government wiretap requests).

When a DPI device cannot identify the application responsible for sending packets by examining the packets' headers and/or payloads, it examines how packets are being exchanged between the computers that are exchanging packets. The device evaluates the spikes and bursts of traffic that occur as the unknown application sends and receives data to and from the Internet, and it correlates the traffic patterns against known protocols that particular programs use to exchange data. This heuristic evaluation effectively bypasses the challenges that data encryption pose to packet inspection devices (full-packet encryption prevents DPI devices from examining payload data).  ISPs are predominantly concerned with network efficiency; as common carriers they are less concerned with the contents being passed along their network and are more interested in *how much* data is crossing their network and *what* is generating that data. Evaluating packets lets ISPs identify applications that might be degrading overall network performance, and lets network administrators develop rulesets that are meant to reduce network congestion.

To make this latter process a bit clearer, let's turn to an example. Skype prevents packet inspection devices from identifying its packets by masking its legitimate packet header information and encrypting payload data. Given that the packets themselves are fully encrypted and the information contained in the headers is bogus, ISPs must adopt a different method for detecting Skype traffic. The solution: DPI devices must watch for a particular exchange of data that occurs when Skype users initiate a voice chat – each time you contact someone using Skype, the seemingly random initial burst of packet exchanges follow a common pattern that can be heuristically identified and correlated with the Skype application (Bonfiglio et. al. 2007). After the application is identified, it is possible to impede or prioritize the packets generated by this application.

Effectively, DPI lets network administrators inspect the totality of unencrypted data exchanges flowing across their network in real time, which enables administrators to stop or manipulate packets before they even leave the originating network or arrive at a recipient within that network. By interrogating packets using DPI devices, system administrators gain greater control over every facet of their network operations.

## 3 - Benefits of Deep Packet Inspection for Network Operators

By examining packet flows at such a detailed level, DPI technologies can be used to improve network security, implement access requirements, guarantee quality of service, and tailor service for particular applications. Network security is improved because system administrators can better inspect data streams to determine if, for example, packets' payloads carry viral payloads or elements of spam email messages. If either kind of payload is suspected, administrators can establish rulesets to prevent the packets from being carried to their destination, and if the point of origin is within the ISP's network then the computer sending the illicit payloads can be temporarily prevented from sending any further packets until they stop sending the packets in question.[7]

This notion of improving network security through data traffic surveillance is accompanied with a drive to generally limit access to the network itself. Because DPI can examine all layers of packet transmissions, it can correlate packets with discrete users who have authenticated to the network; if a packet cannot be correlated with a known authenticated user, the packet can be prevented from escaping the ISP's network perimeter, and network administrators can investigate who is attempting to use their network without first authenticating.

Quality of service, as it pertains to DPI, focuses on the ability to limit the transmission of packets that might degrade overall network performance; by streaming large amounts of data for an extended period of time, a user might use a large amount of bandwidth and upset other users' experiences on the network. To improve quality of service, DPI devices target 'problem' applications and packet-types by either reducing their priority level (i.e. they let all other packets travel along the network before the 'problem' packets) or preventing them from being transmitted or received.

Finally, DPI devices let network operators guarantee certain levels of service to different users. As an example, ISPs can ensure that if you purchase a Voice over Internet Protocol (VoIP) plan or a fast BitTorrent plan, that your VoIP or BitTorent packets will be given

[7] Presently, this often means that ISPs will temporarily disconnect users from accessing the ISPs network (and thus the Internet at large). Rogers Communications often does this. When users call their ISP's customer service department the representatives inform the customers of the illicit packets and explain how to stop transmitting them, after which the customer is reconnected to the ISP's network.

priority on their network. If the customer does not purchase one of the ISPs premium plans, however, they might experience slow delivery speeds (and lost packets), which limits the ability to have a conversation over VoIP or to receive and send data at the maximum theoretical speeds provided by BitTorrent applications.

## 4 – Questions of Deep Packet Inspection and Surveillance

DPI devices enhance network operators' control over the traffic flowing across their network. These enhancements come through the heightened capacity to survey data flows at both broad and particular levels. Rather than suggesting that these are the comprehensive, or necessary, levels of analysis for DPI-enabled surveillance, I approach surveillance from these perspectives to draw attention to fields of inquiry that can be taken up in subsequent research.

In attending to surveillance at a broad level of social analysis, David Lyon notes that surveillance is "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or detection" that it is "deliberate and depends on certain protocols and techniques" (Lyon 2007: 14). Lyon's definition corresponds with potential uses of DPI technologies to influence action though the alteration of data packets, and management of action by potentially limiting websites that can be visited and online actions that can be performed. Further, the use of DPI to secure networks against viruses, and need to perform regular analysis of packets to detect heuristic matches and anomalies, corresponds with Lyon's definitional elements of 'protection' and 'detection'. This having been said, it is questionable whether or not DPI devices are *generally* used for all of these purposes by the particular companies that are deploying DPI devices in their network infrastructures – future research is needed to identify how *particular* uses of DPI technologies might correspond with facets of Lyon's definition to tease of the subtleties of DPI-enabled networking practices.

It is important to distinguish between surveillance, which is evidenced when ISPs use DPI devices to inspect each packet that passes along their network, and search, which entails looking for a particular element of network traffic. Surveillance extends beyond search because "[r]ather than targeting specific information, surveillance can ensnare a significant amount of data beyond any originally sought" (Solove 2008: 109). In making this distinction, Solove is calling attention to potential breadth of digital surveillance, while also implicitly identifying that there is a qualitative difference between broad-based social surveillance, and individual surveillance or particular searches for information. While broad surveillance may accidentally capture information beyond that sought, 'search' surveillance – the specific targeting of an information-type – may provide the surveying party with a deep field of data that is relatively limited in its scope. Whereas broad surveillance may identify how popular VoIP applications are on an ISP's network, a targeted search of a customer's Internet habits may reveal precisely how much that individual uses such applications. The distinction between broad and narrow surveillance processes raises questions of the felt and realized impacts of surveillance, and whether multifaceted responses to different calibers of surveillance are needed when addressing ISP uses of DPI equipment. In both broad and narrow surveillance procedures, questions of who is, or may be, discriminated against must also be raised, as must the possibilities of 'social sorting' that may arise following the deployment of DPI technologies.

In an era where communications are increasingly digitized, the capacity to investigate content as well as who is talking with who, for how long, and along particular mediums is incredibly valuable; "[t]raffic analysis reveals an organization's structure, its membership, even the roles of its members." (Diffie and Landau 2008:309). DPI enables ISPs to identify the tools that are being used to communicate (e.g. VoIP, instant messaging clients, etc) in addition to the IP addresses that communications data is being transmitted to, number of intended recipients of data flows, and the perceived relations between individuals transmitting data to one another. Though it is possible to construct vast social network maps, with DPI technologies used to contextualize these maps by analyzing and/or capturing unencrypted data packets, I do not mean to suggest that Canadian ISPs *are* developing widespread social organization maps – to date there is no evidence to support such a claim. The ethical (and legal) restraint demonstrated by ISPs does not, however, mean that they could not use DPI technologies for extensive communicative and social surveillance.

ISPs in Canada are presently using DPI technologies to monitor and shape bandwidth, as was evidenced in the complaint that the Canadian Association of Internet Providers (CAIP) filed with the CRTC about Bell Canada's traffic shaping policies (CRTC 2008). Per that complaint, Bell actively uses DPI devices to regulate packets that are generated by file-sharing applications, such as BitTorrent. Bell's regulation of BitTorrent packets affects packets sent along their ADSL subscriber lines, including CAIP's customer base. Rogers Communications uses DPI alter data flows that customers receive. Rogers modifies webpages to announce to their customers that they are approaching their allocated monthly bandwidth (Bangeman 2008), as well as to redirect customers to Rogers' own webpages when customers incorrectly type a Internet address in their browser (Geist 2008).

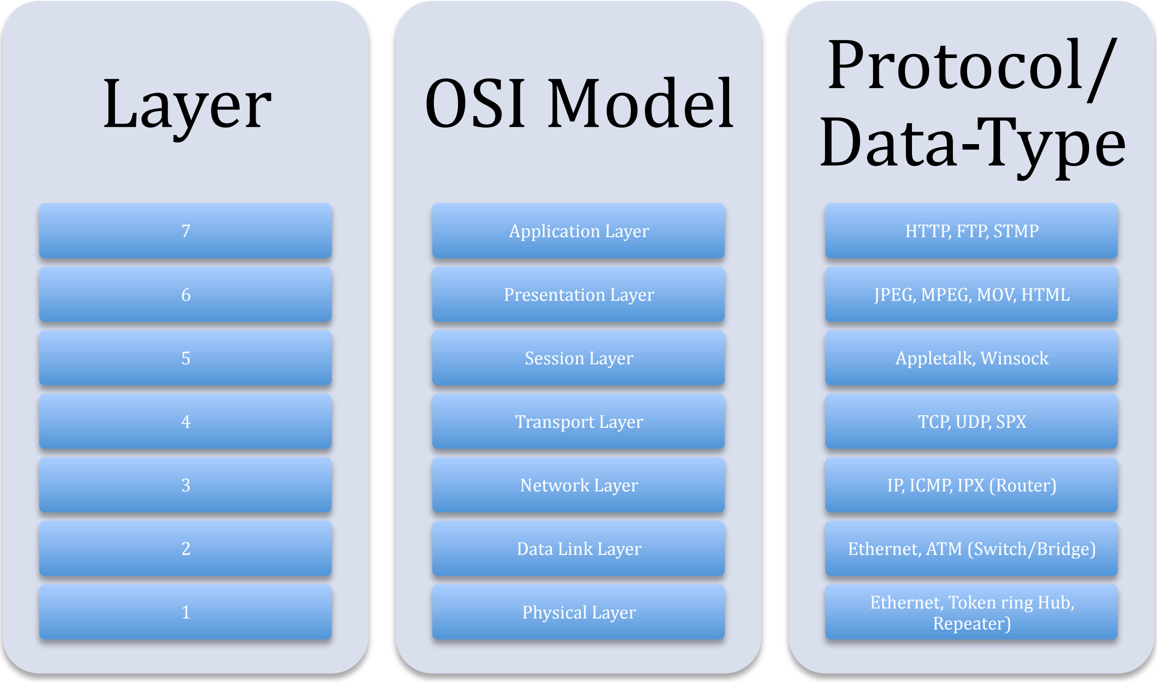
As evidenced these cases, Canadian ISPs are using DPI technologies to survey the entirety of their clients' activities as part of their routine business operations. They are not just searching for particular information, but instead use a massive surveillance technology to comprehensively remain aware of the data traffic coursing along their respective networks. These ISPs are moving beyond just monitoring data flows using DPI – their willingness to alter data flows demonstrates that they are enforcing particular norms that they hold about proper and improper uses of their networks. In Bell's case, customers are being (implicitly) 'taught' that some software applications should not be used during certain hours of the day, and in that of Rogers' customers they are 'learning' that it is permissible for ISPs to change how (and whether) websites appear to customers. DPI has not, however, been evidently used to 'dig deeply' into the packet streams of particular Canadian beyond routine analysis and injection routines – there is no evidence that Canadian ISPs have shifted from surveillance to search.

## Conclusion

The use of packet inspection technologies is not new, and they are an important element of network operations for any company that maintains a substantial networking infrastructure. DPI technologies realign ISPs' capacities to survey and modify data flows by virtue of their awareness of the entirety of packets' compositions as they pass through ISP networks. Whereas SPI and MPI technologies enable administrators to stop content from reaching clients, and let them to record packet information, the advent of DPI technologies restructures the possible range of surveillance that ISPs' clients may be subject to. The normative evaluation of statements and communication protocols, and insertion of coherent corporate statements into data flows, raises free speech, privacy, surveillance, network neutrality, and freedom of association concerns. While it is beyond the scope of this paper to address these broader concerns, subsequent research into the relationships between DPI and these issues must take place to better understand the consequences and implications of current ISP packet inspection technologies and their associated practices.

## APPENDIX I – Protocols/data-types and the OSI model

While the OSI model is used to broadly divide the composition of packets, various protocols are involved at varying layers of packets. The figure below provides a listing of various protocols in relation to the OSI model to assist readers in isolating what protocols packet inspection technologies can identify and monitor.



| Layer | OSI Model | Protocol/ Data-Type |
|---|---|---|
| 7 | Application Layer | HTTP, FTP, STMP |
| 6 | Presentation Layer | JPEG, MPEG, MOV, HTML |
| 5 | Session Layer | Appletalk, Winsock |
| 4 | Transport Layer | TCP, UDP, SPX |
| 3 | Network Layer | IP, ICMP, IPX (Router) |
| 2 | Data Link Layer | Ethernet, ATM (Switch/Bridge) |
| 1 | Physical Layer | Ethernet, Token ring Hub, Repeater) |

**Figure 5: Protocols/data-types and the OSI model**

## 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 October 10, 2008. URL: http://arstechnica.com/articles/culture/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 (2008). “Rogers latest ISP to “Help” customers with DNS redirects,” *ArsTechnica*. Published July 20, 2008. Last accessed October 21, 2008. URL: http://arstechnica.com/news.ars/post/20080720-rogers-latest-isp-to-help-customers-with-dns-redirects.html

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

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.

CRTC (2008). *Telecom Decision CRTC 2009-108: The Canadian Association of Internet Providers’ application regarding Bell Canada’s traffic shaping of wholesale Gateway Access Service*. Ottawa: Government of Canada. URL: http://www.crtc.gc.ca/archive/ENG/Decisions/2008/dt2008-108.htm

Diffie, Whitfield and Susan Landau (2008). *Privacy On the Line: The Politics of Wiretapping and Encryption (Updated and Expanded Edition)*. Cambridge, Mass.: The MIT Press.

Geist, Michael (2008). “Rogers Implements New Approach On Failed DNS Lookups.” *Michael Geist* (Blog). Published July 18, 2008. Last accessed October 20, 2008. URL: http://www.michaelgeist.ca/content/view/3199/1/#akocomments_comments_start

Gudea, Sorin W. (2004, February). *Media Richness and the Valuation of Online Discussion Support Systems*. Paper presented at the *Seventh Annual Conference of the Southern Association for Information Systems*, Savannah, GA.

ipoque GmbH (2008). *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

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

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.

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

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.

## References

DiNolo, Dan (2004). "Understanding Network Models – The OSI Model," *Network Newz: For Networking Professionals*, Published January 22, 2004. Last accessed October 10, 2008. URL: http://tinyurl.com/3ccfza.

Microsoft Help and Support (2002). *Q103884: The OSI Model's Seven Layers Defined and Functions Explained*. Published February 27, 2002. Last accessed October 10, 2008. URL: http://support.microsoft.com/kb/103884