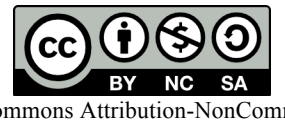
Literature Review of Deep Packet Inspection:

Prepared for the New Transparency Project's Cyber-Surveillance Workshop

by Christopher Parsons*

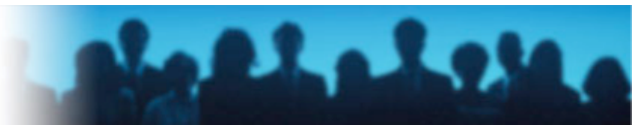
Abstract

Deep packet inspection is a networking technology that facilitates intense scrutiny of data, in real-time, as key chokepoints on the Internet. Governments, civil rights activists, technologists, lawyers, and private business have all demonstrated interest in the technology, though they often disagree about what constitutes legitimate uses. This literature review takes up the most prominent scholarly analyses of the technology. Given Canada's arguably leading role in regulating the technology, many of its regulator's key documents and evidentiary articles are also included. The press has been heatedly interested in the technology, and so round out the literature review alongside civil rights advocates, technology vendors, and counsel analyses.



Version 4.1 : March 6, 2011

* PhD Candidate in the Department of Political Science at the University of Victoria. Christopher is presently funded through the Social Sciences and Humanities Research Council (SSHRC) and had earlier research funded through the New Transparency Project and the Office of the Privacy Commissioner of Canada's Outreach Program. He thanks Joyce Parsons for her editorial assistance.



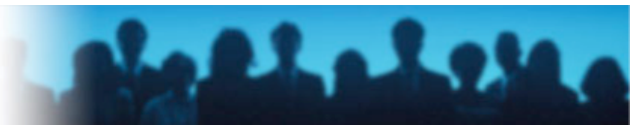
Introduction

We are amid a standardization revolution, a mass translation of discordant analogue signal types into interoperable digital transmission standards. Speech, writing, and video now traverse the globe at near light-speeds via spiderlike networks of fibre-optic cables, and all of this digitized consumer traffic to and from the Internet passes through Internet Service Providers' (ISPs) gateways. ISPs, as communicative bottlenecks, are ideally situated to monitor, mine, and modify data using the deep packet inspection (DPI) appliances situated within their networks. Around the globe, communications are mediated by DPI equipment in service of the respective interests of ISPs, advertisers, governments, and copyright lobbies.

DPI's broad capacities—and the attention given to the technology by the above-mentioned actors—have piqued the interest of researchers in various fields of the social sciences. Common questions are beginning to emerge, including: Who is driving deep packet inspection? What is DPI's role in network management? How (and why) have copyright lobbies, advertisers, and government taken an interest in monitoring data communications? What uses of the technology are considered legal, and in what cases are privacy interests endangered by the technology?

In addition to formal academic literature, government regulators have commissioned reports and essays to explore the possible implications and future directions of the technology. These commissioned documents have been supplemented by formal regulation in some jurisdictions, perhaps most prominently in Canada. Journalists, particularly those on 'DPI-beats', are responsible for influencing ongoing discussions about the technology (and its associated politics), with their accounts often supplemented by publicly accessible legal analyses, advocacy regulatory filings, and vendor white papers.

This literature review reflects the variety of scholarly interests associated with DPI technology, commissioned government reports and key journalist accounts, as well as



select publications by counsel, civil rights advocates, and vendors. I also address major Canadian regulatory decisions that are (at present) minimally accounted for in scholarly literatures. The inclusion of nonacademic sources is deliberate: government documents identify empirical sources scholars will likely integrate into the literature over time, vendor statements provide useful insight into their own understanding of the technology's future, and advocates often demonstrate how well (or poorly) academic research has been disseminated into policy networks. Thus, in examining these sources, academics might recognize where DPI is moving within policy spheres, as well as how past publications have been integrated into informed public discourse.

In summary, this literature review addresses some of the motives and strategies of digitally mediated surveillance actors, relationships between actors involved in DPI-based surveillance, the politics of DPI, the impact of DPI on personal privacy, and how novel technical configurations promote surveillance and challenge privacy. Prior to examining the literature itself, however, I briefly discuss how DPI functions as a technology and introduce the reader to some of the technical terminology associated with it.

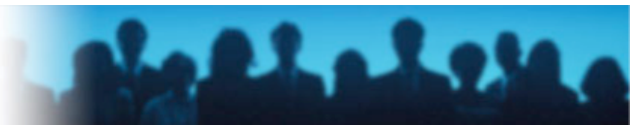
Deep Packet Inspection 101

Deep packet inspection is a networking technology that businesses and Internet Service Providers use to monitor what applications are generating and receiving network traffic. Data flows across the Internet as packets, and these packets are composed of two key elements: headers and payloads. The header directs packets to their terminal destinations, like an address on a postcard directs to postcard to the recipient's address. The payload holds the packet's actual contents; using the postcard metaphor, the payload holds the image, text, color of the text, handwriting style, and so forth. Whereas earlier networking technologies analyzed and filtered packets based on header information, DPI systems permit a more granular analysis of packets based on their payload. Further, DPI can modify the contents of packets and identify data traffic even when it is encrypted. Examining the content of communications—whether they be unencrypted or not – and then acting on communications by modifying them, accelerating them, or decelerating them based on privately developed policies has led to considerable controversy amongst Internet governance scholars, government regulators, civil rights advocates, and lawyers.

Scholarly Analyses of Deep Packet Inspection

Mueller, Milton (2010). *Networks and states: The global politics of Internet governance*. Cambridge, Mass.: The MIT Press.

Networks and States focuses on how information and communication systems are



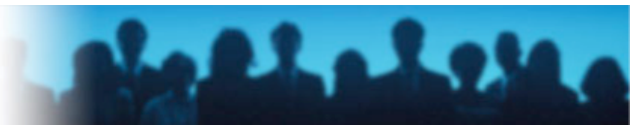
developed on the global stage. Mueller argues that scholars should focus on institutions and their forms, rather than digital code, because changes at institutional levels comprehensively address Internet governance issues such as intellectual property management, security, content regulation, and critical Internet resources (e.g. IP addresses and domain name registries). By focusing on governance structures we can understand who is advocating for DPI's use whereas code analysis limits our insight into the politics of Internet governance. Such focus is especially needed when examining security and content regulation, given that both are attentive to DPI's capabilities to scan, sort, classify, border, and censor communications using automated decision sets.

Resisting calls that legitimize any and all national controls the Internet, Mueller maintains that nation-states must be situated within the framework of denationalized liberalism. This framework limits states to "those domains of law and policy suited to localized or territorialized authority" and favors "a universal right to receive and impart information regardless of frontiers, and sees freedom to communicate and exchange information as fundamental and primary elements of human choice and political and social activity" (269). Denationalized liberalism is supplemented by neo-democratic rights, which recognize nations' role(s) in some governance decisions while ascribing individuals "formal rights and representational status within the institutions that govern them so that they can preserve and protect their rights as individuals." Effectively, this would let individuals determine how information should be mediated and empower them to prevent deployments of DPI that unilaterally, at state request, limit access to information on non-(neo)democratic grounds.

Bendrath, Ralf (2009). Global technology trends and national regulation: Explaining variance in the governance of deep packet inspection, presented at the International Studies Annual Convention (February 2009). Retrieved from http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf

Whereas much of the Internet governance field focuses on institutions responsible for directing technological developments online (e.g. ICANN) and how devices that connect to the network are (dis)abled (e.g. Zittrain, Lessig), Bendrath examines the middle of digital networks. Specifically, he conducts a technically aware policy analysis that links the specifics of deep packet inspection as a technology to the particularities of social and political policies. As such, he remains aware of the technology's characteristics and the social and political contexts in which it is embedded. By examining how these fields interact, he evaluates the co-constitutive nature of technology, politics, and policy, and prevents a deterministic perspective from driving his analysis.

Bendrath considers a series of issues when evaluating how governance differences emerge from among actors' interests. Using case studies focused on network security, bandwidth management, ad injections, copyright content filtering, and government



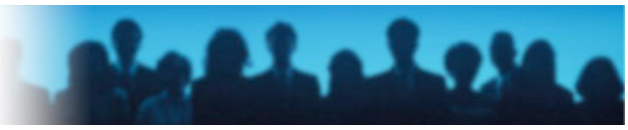
surveillance, we see that DPI lacks a deterministic function: in varying jurisdictions, actors mediate its actual uses by influencing the technology's deployment. Using these case studies, Bendrath argues that technology-oriented policy analyses help explain variation across DPI's use-cases. Further, his approach recognizes the role of norms and institutions where interactions between policy and technology take place. As a result, he can explain variations of DPI's actual implementation across similar use-cases (e.g. copyright enforcement). Finally, by recognizing the role of actors, he can acknowledge particular judgment errors and failed gambits that, when integrated into institutional analyses, improve the precision of policy analyses addressing DPI and other fungible technologies.

van Schewick, Barbara (2010). *Internet architecture and innovation*. Cambridge, Mass.: The MIT Press.

van Schewick examines "how changes in the Internet's architecture (that is, its underlying technical structure) affect the economic environment for innovation," evaluating the impact of those changes from a public policy perspective (2). She traces the economic consequences of shifting from an Internet structure that lets any innovator design applications or share content, to one where ISPs approve access to content and design key applications in-house (e.g. P2P, email). DPI systems are key in enabling this latter mode of network control, and many ISPs prefer it to an Internet they do not control.

van Schewick distinguishes two versions of the "end-to-end" principle. The narrow version permits network owners to interfere in an application's processes when the interference is classified as "performance enhancement." The broad version asserts that functions and services "should be carried out within a network layer only if it is needed by all clients of that layer, and it can be completely implemented in that layer" (58). She argues that deviating from the broad version, such as by using DPI to modify applications' packet transfers, negatively affects innovation by empowering network controllers to influence or block certain applications and content from passing over their networks.

After an extensive economic and technical analysis of information networks, she concludes that citizens and their representatives must understand the impacts of the Internet's architecture for the future of communication and innovation. ISPs are intent on better controlling and monetizing their networks, but to secure short-term profits they are endangering the Internet's long-term evolution. Given citizens' reliance on digital communications, they must interrogate such issues and force ISPs to operate for the public good.



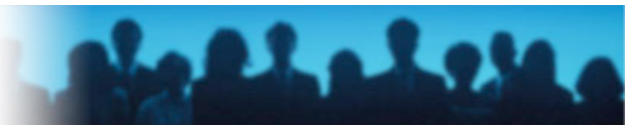
Bendrath, Ralf & Mueller, Milton. (2010). *The end of the Net as we know it? Deep packet inspection and Internet governance*. Working paper series, SSRN. Retrieved August 10, 2010 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1653259

This paper examines how DPI could end the Internet's existence as an open network. Its authors argue that scholars must study relationships between DPI, governance structures, and social interactions to adequately account for the technology's potential impacts on the Internet's future configuration. By focusing on these relationships, institutional actors and environments are accounted for, which creates a foundation upon which scholars can conduct sustained evaluations of DPI.

Recognizing that "technological changes do not determine social interactions," the authors acknowledge that such changes do "have distinctive effects that are derived from the way their unique capabilities interact with the interests of specific actors and the institutional environment" (3). DPI, as a disruptive technology, challenges end-to-end arguments, threatens political freedoms, and upsets the Internet's economic openness. Given the multivariate potentialities of the technology and how easily it integrates with various institutions' and actors' policy objectives, Bendrath and Mueller argue for adopting a theory of technology/society co-production to link "the concrete characteristics of DPI technology to specific actor constellations, modes of interaction and institutional settings" (23). As a result, DPI is seen as "an input into a socio-technical regime" to explain variance within and across DPI use-cases. In light of variances, the authors avoid concluding that the Internet will necessarily become a closed system; instead they assert that today's citizens can shape the Internet's future configuration.

Cooper, Alissa (2010). The singular challenge of ISP use of deep packet inspection. *Deep packet inspection Canada*. Retrieved from http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection/

DPI raises privacy issues because ISPs deploy it at key chokepoints in their Internet infrastructure, because the costs to users of switching ISPs are high, and because of the technology's propensity for mission creep. While many parties can potentially investigate digital communications, none have access to communications on the scale of ISPs; all communications must pass through ISPs' networks in transit between Internet-connected computers. This affords ISPs, and actors influencing ISPs, the potential to monitor all data traffic. While consumers may voice concerns about DPI usage, their ability to switch to a non-DPI using provider may be limited. High costs (stemming from the loss of savings associated with telecommunications bundles of phone, Internet, and mobile services), potential requirements for new hardware, and the need to learn a new billing regime all restrict consumers' ability and willingness to switch providers—even in



situations where competition between ISPs is relatively prolific. Finally, DPI's fungibility lets ISPs deploy it for one reason, such as enhanced billing possibilities, and then repurpose it for others, such as throttling particular traffic or modifying data packets in real time. Given the potential for deep packet inspection technologies and vendors' aim of making the technologies invisible, they constitute particularly significant privacy risks that must be addressed through regulatory or legal processes.

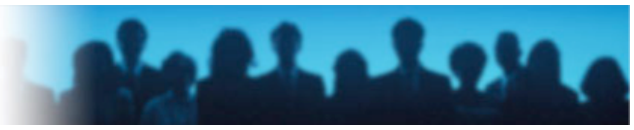
Daly, Angela. (2010). The legality of deep packet inspection. Presented at the First Interdisciplinary Workshop on Communications Policy and Regulation "Communications and Competition Law and Policy—Challenges of the New Decade." Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024

Daly is concerned with how DPI could be used to harm Internet users. After briefly describing the technology, she notes its most commonplace uses: network security, government surveillance, network management, targeted advertising, and governing copyright infringement. The process by which these uses take place—the analysis of payload content of data packets—raises a series of legal issues. Specifically, examining the content of communications runs contra to the 4th Amendment rights in the United States and Article 8 of the European Convention on Human Rights that regulates the processing of personal data. Free expression is jeopardized because ISPs mediate communications based on protocol and packet analysis and prioritize certain expressions over others. Prioritization is closely related to competition worries, where ISPs might prioritize their own "legitimate" content services to the detriment of competitors who may be transmitting copyright infringing data to end-users.

Daly proposes a series of responses: ISPs should have to inform customers of how the technology is used, though she admits that simple disclosures do not necessarily eliminate privacy violations, competition worries, or other potential harmful uses of the technology. To address competition worries, *ex ante* rules may be required to avoid stifling innovation. Finally, to maintain a vigorous public sphere, governments might impose free speech requirements upon private communications networks to offset DPI systems' potential censorial capacities.

McKelvey, Fenwick. (2010). Ends and ways: The algorithmic politics of network neutrality. *Global Media Journal - Canadian Edition*, 3(1). 51-73.

McKelvey locates DPI at the intersection of competing algorithmic understandings of the Internet, specifically those algorithms that are in service of end-to-end principles (packets are transmitted from point to point on a best effort basis, without the Internet's



infrastructure understanding their content) and those guaranteeing Quality of Service (the Internet's infrastructure can identify and prioritize particular packets based on actual or inferred content) provisions. Algorithms operate as a combination of logic and control, and possess a politics because "they distribute and finalize network resources to transmit packets" (57).

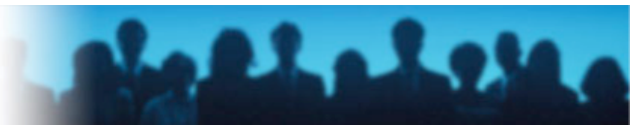
DPI accelerated the evolution of Quality of Service algorithms, letting ISPs create tiered service offerings that accelerate or delay application traffic. Such offerings are possible because DPI affords privilege to the core of the network. Such privilege puts network neutrality—a position privileging ends—against the interests of ISPs that are often proponents of managed services. Rather than advocating for the dominance of either network algorithm, McKelvey suggests that the real question is how to integrate the two and develop a robust Internet. This said, he argues that if network neutrality advocates fail to acknowledge their approach's normative facets and that its political character derives from the potential to (re)structure democratic openness, they will lose out to the economic interests favoring core-centric, quality-of-service dominated algorithmic politics.

Macia-Fernandez, Gabriel, Wang, Yong, Rodriguez, Rafael & Kuzmanovic, Aleksander. (2010). ISP-Enabled Behavioral Ad Targeting without Deep Packet Inspection. Proceedings of IEEE Infocom 2010 (March 2010). Retrieved from http://networks.cs.northwestern.edu/publications/adver.pdf

The authors recognize that using DPI to inspect and modify payload contents for behavioral advertising purposes is likely illegal. In light of this, they suggest a method whereby ISPs can avoid using DPI but still perform behavioral advertising. Importantly, the authors suggest that their methodology can be performed with or without subscriber consent, whereas DPI-based advertising (in the United States) requires consent because it constitutes a form of wiretapping.

The process that Marcia-Fernandez et al. propose involves crawling websites and deriving statistical information about them. Then, they suggest that ISPs extract nonpayload-based information from subscribers' browsing sessions at ISP network points and correlate information between these two data sets to identify subscribers' browsing patterns. Their technique results in an average successful identification rate that is as high as 86 percent with false positives generated 5 percent of the time. Success rates diminish slightly when users either intentionally act to obscure their HTTP traffic or where a NAT firewall hinders the separation of discrete user data flows.

Given the source of these analyses and the manner in which webpages are statistically identified, it is challenging for endpoints (i.e. Internet subscribers and website hosts) to defend against this method of analysis, save by routing data traffic through third-party services (i.e. proxies) or randomizing elements that generate the webpage's statistical profile. What the paper demonstrates is that limiting uses of DPI will not necessarily limit



ISP surveillance of subscriber habits, whereas regulating behavior may. Actions, not technologies, need to be subject to regulatory oversight.

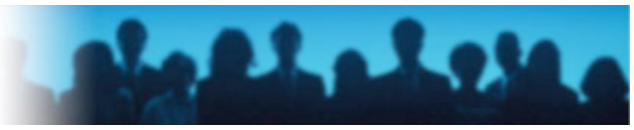
Ohm, Paul. (2008). The rise and fall of ISP surveillance. *University of Illinois Law Review* 1417.

Ohm asserts that we should focus on individual harms stemming from surveillance and recognize that technological, economic, and ethical forces all point towards a "storm of unprecedented, invasive ISP monitoring" (4). He maintains that ISPs oversell their ability to anonymize collected data, that providers' claims of needing to more deeply inspect content are suspect, and that we should distrust suggestions that users and ISPs have entered consensual agreements around DPI-based surveillance. To determine the risk of individual harms stemming from surveillance, ISPs and regulators should adopt a three-step process that asks how sensitive is the information at risk, whether there there been harmful breaches in the past and if so, requires policymakers to make predictions about the future.

Critically, "anonymity cannot effectively address the harm to the sense of repose. The harm comes from the fear that one is being watched. It can result in self-censorship. It is not the kind of harm that is easily offset by hypertechnical arguments about encryption and one-way hash functions" (49). Thus, novel surveillance systems like DPI must be (largely) restricted to preventing hacking and viral outbreaks and traditional monitoring systems that cannot capture personal information relied upon for network management. Most importantly, Ohm argues that privacy, freedom, liberty, and autonomy must be introduced into the otherwise technocratic discussions of network neutrality and management to ensure that ISPs' networks facilitate these key democratic values.

Parsons, Christopher. (2010). Moving across the Internet: Code-bodies, code-corpses, and network architecture. *CTheory: Theory, Technology, and Culture* 33(1). Retrieved from http://www.ctheory.net/articles.aspx?id=642

How does interrogating data packets and attempting to rend packets' meaning based on communications protocols and technical signatures impact digital embodiment? In exploring this question, Parsons theorizes the existence of a code-body, which is composed of organs (the protocols that act as digital circulatory systems), orifices (the applications that eat or excrete data), and meanings (the truths and values made manifest through the interaction of organs and orifices) that are presently in confrontational relationships with DPI appliances. The rise of technologies that deeply inspect packets at key Internet chokepoints promotes the use of encryption, which functions as an



exoskeleton that secures the code-body from undue surveillance. This securitizes what was previously a naked, or unencrypted, existence.

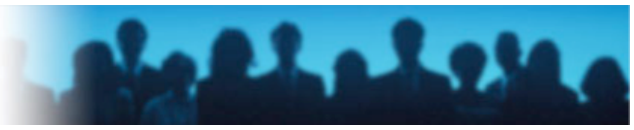
The code-body is juxtaposed against DPI devices that behave as code-corpses. Such devices move through networks in a "programmatically fixed, zombie-like fashion," processing, evaluating, and acting upon particular body-types while being forever frustrated from perceiving the meanings that link organs and orifices. Parsons suggests that this frustration is manifest as a kind of Derridean haunting that ultimately scars the code-body. The hauntedness of the corpse means it can never fully understand the body, but, regardless, the corpse mediates the code-body's identity performances: carapaces are developed, (data) mobility is hindered, and potentialities are forcibly modified against the body's will.

Sandoval, Catherine J. K. (2009). Disclosure, deception and deep packet inspection: The role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the net neutrality debate. *Fordham Law Review (78)*, 641.

American ISPs have deployed technologies like DPI since being relieved of common carrier provisions in 2005. Sandoval argues that customers cannot understand what might negatively impact their Internet service, ISPs demonstrate limited technical and policy transparency, and little consumer awareness exists concerning privacy policies and service policy restrictions. To protect consumers, regulators must investigate ISPs and determine whether they are engaging in deceptive conduct (an issue for the Federal Trade Commission (FTC)) and whether application discrimination violates the Communications Act (an issue for the Federal Communications Commission (FCC)).

Sandoval maintains that US regulatory bodies possess sufficient grounds and legal power to scrutinize ISPs' practices. While ISPs may not be violating their contracts with consumers, information about DPI's usage is not transparent to their subscribers. Without meaningful awareness, customers cannot understand the nature of their service. The FCC must evaluate whether transparency is required and if application discrimination is permitted under the *Communications Act*. If the FTC and FCC actively regulate the conditions under which Internet services are sold and require ISP transparency concerning DPI's use, a stronger competitive landscape between ISPs, which could compete on the grounds of (not) using DPI, might arise. However, transparency is not entirely sufficient. ISPs have demonstrated a willingness to control application traffic; to protect consumers from deceptive practices (and innovation more generally), regulators must ensure that the threat of anti-competitive investigations hangs over ISPs' heads.

Wagner, Ben. (2oo8). Deep packet inspection and Internet censorship. Presented at 3rd



Annual Giganet Symposium (December 2008). Retrieved from http://advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/

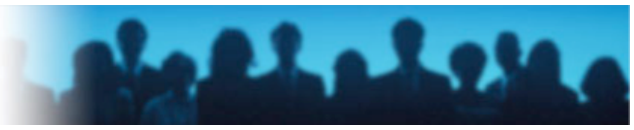
Many concerns about DPI relate to commercial applications of the technology, but Wagner argues that we should focus on how governments use the technology to promote widespread censorship. Being transparent about DPI's use might be a sufficient means to protect citizens where their speech is already constitutionally secured, but many states have a vested interest in limiting speech. As a result, transparency is not necessarily a panacea to limit "bad" deployments of the technology; something more must be demanded.

Wagner discusses how DPI facilitates subtle mediations of content that states find offensive. For example: whereas China presently blocks entire websites (e.g. bbc.co.uk) DPI lets censors selectively modify particular strings of text. As a result, end-users might never know that the BBC had been edited by the state. While a global network neutrality norm—the position that intermediaries should only transit, and not interfere with, data traffic—might alleviate censorship concerns, Wagner doubts such a norm will develop in the near future. Thus, technical measures such as encryption and steganography need wide distribution and must be accompanied by international agreements on appropriate uses of DPI. Without such agreements and standards, there will be no normative measure to weigh "good"and "bad" uses of DPI, and thus advocates and academics alike will be unable to normatively evaluate the use of the technology.

Wu, Tim. (2010). *The master switch: The rise and fall of information empires.* New York: Knopf.

Will the Internet remain open or will corporate and government interests change its character as with previous communication mediums? This question underlies *The Master Switch*. Wu traces the history of radio networks, the telephone, broadcast TV, and Hollywood to argue that there is a cycle to American communication networks. Specifically, they progress from "somebody's hobby to somebody's industry; from jury-rigged contraption to slick production marvel; from a freely accessible channel to one strictly controlled by a single corporation or cartel—from open to closed system" (6). By examining the history of information-communication systems, he argues we can foresee the Internet's possible fates.

Much of the book turns on Schumpeter's cycle of industrial life and death, along with an analysis of how law sustains dying industries and stymies technological development. The danger associated with communication technologies becoming closed—controlled by



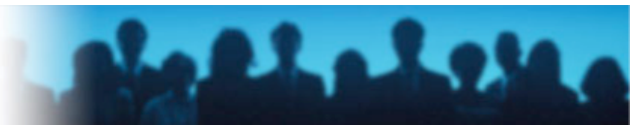
a relatively homogeneous group—is that such homogeneity confers a "master switch" to the owners and lets them limit information availability and platform innovation. To prevent an Internet master switch, Wu calls for a Separation Principle. This principle would "divide *all* power that derives from the control of information" (304), keeping various "layers" of delivering and producing information separate while limiting government from promoting network monopolies, technologies, or integrations of key information economy functions. Such a principle would limit ISPs' abilities to (de)prioritize data, an ability they currently use to their competitive advantage, while, at the same time, limiting government surveillance programs that depend on ISPs acting as chokepoints for the Internet.

Deep Packet Inspection and the Canadian Government

Finnie, Grahm. (2009). ISP traffic management technologies: The state of the art. Report for the *CRTC Public Notice on the Review of the Internet traffic management practices of Internet service providers*. January 2009. Retrieved October 21, 2010 from http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm

ISPs have traditionally over-provisioned sections of their network to enable a high quality of service during times of high network usage. With the growth of over-the-top services (e.g. Hulu, YouTube, Netflix) and widespread uploading of content, ISP networks threaten to be overwhelmed. As a result, ISPs are deploying DPI systems of differing complexity levels to differentiate between applications' data traffic and improve customers' quality of service based on their monthly data subscriptions.

In developing his report, Finnie finds that DPI vendors compete on the number of protocols that can be detected, speed at which the devices can analyze data traffic in real time, number of subscribers that single devices can parse, and ability to address security threats such as distributed denial of service (DDoS) attacks. To date, most traffic management operates without direct reference to particular subscribers, though this is changing. Present technology facilitates a shift from protocol- or application-specific policies to subscriber-centric approaches, and DPI will form a backbone for many subscriber management systems. Such management systems will likely be integrated with federated identity schemes, where logging into one device or portal will either enable a series of devices to access online environments or enable the subscriber on a single device to access multiple online environments without needing to log into each one separately. Finnie concludes by noting that DPI might affect future Internet standards, but he avoids stating how those standards might actually be affected.



Clarke, Roger. (2009). Deep packet inspection: Its nature and implications. *Office of the Privacy Commissioner of Canada Deep Packet Inspection Essays Website*. Published March 11, 2009. Retrieved December 10, 2010 from http://dpi.priv.gc.ca/index.php/essays/deep-packet-inspection-its-nature-and-implications/

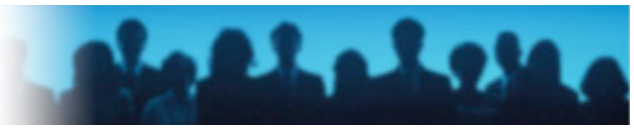
In this essay, prepared for the Privacy Commissioner of Canada, Clarke outlines the technical characteristics of DPI and its welcome and unwelcome uses. Technically, DPI transforms intermediary nodes in a network—nodes needed to forward packets to their destinations—into sites that investigate more data than required to transmit a packet to its destination. In some cases, individuals may consent to intermediary nodes examining deep-nested elements of data packets—limiting spam, virus-ridden messages, or access to particular websites may be appreciated. Further, inspection at intermediary nodes might be used to establish network caches, which could provide faster access to requested data.

Other instantiations of DPI may be less desirable. Individuals would presumably resist widespread use of DPI to monitor data transmissions and collect secret information (e.g. credit card numbers), to let law enforcement survey data communications, to modify messages in transit, or to block access to information based on analyses of message content. In each of these use-cases, consent is rarely given, and thus justification, access controls, and enforcement measures must be established before using the technology. Clarke concludes on a pessimistic note: the present status of the technology's deployment by ISPs indicates that abuse of the technology is prevalent, with such abuses simultaneously endangering the Internet's basic infrastructure and civil rights.

Canadian Radio-television and Telecommunications Commission. (2009). *Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers*. October 21, 2009. Retrieved August 19, 2010 from http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm

This policy follows from a complaint that accused Bell Canada of inappropriately using DPI equipment to slow some wholesale ISP customers' data traffic. In the complaint, Bell asserted that DPI should be permitted because exclusively investing in network volume capacity was an untenable long-term solution for network management problems. The CRTC agreed, though ordered that Bell's wholesalers should not experience more stringent packet delays than Bell applied to their own retail customers. The regulatory body also noted that it would launch a larger proceeding concerning Internet Traffic Management Practices used by Canadian ISPs. The result of that larger proceeding is Regulatory Policy CRTC 2009-657.

Policy 2009-657 identifies how national carriers can utilize DPI for traffic management. They must publicly document why, when, and what type of traffic is being managed, who



is affected, and how the practice(s) affect subscribers' Internet experience. Changes to practices must be announced 30 days before the change occurs for either retail or wholesale customers. While DPI can collect personal information about ISPs' subscribers, this order prevents ISPs from using the information for anything other than traffic management, thus limiting (or at least delaying) function creep. Finally, DPI cannot be used to block particular content, and data traffic cannot be delayed, without prior CRTC approval, to an extent that it would influence the content or meaning of the transmission. This policy is widely referenced by civil advocates and foreign regulatory bodies, all of whom are regularly incorporating the CRTC's decision their own analyses of how DPI should(n't) be regulated.

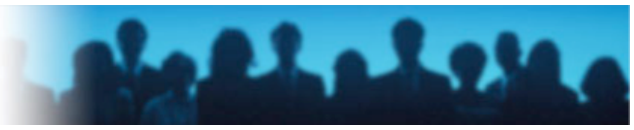
Office of the Privacy Commissioner of Canada. (2009). *Report of Findings: Assistant Commissioner recommends Bell Canada inform customers about deep packet inspection*. September 2009. Retrieved January 20, 2011 from http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm

This report follows from a complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC). CIPPIC alleged that Bell Canada used DPI to collect and use personal information from customers without their consent; collected and used more personal information than necessary to ensure network integrity and service quality; and failed to adequately notify customers about Bell's use of DPI. The commissioner found that Bell's use of the technology for network management needed to be clarified in service agreement policies, that Bell had to better organize information about the technology on its website, and that Bell needed to develop a Frequently Asked Questions page to explain DPI to customers. Finally, the Commissioner's office found that the system collected personal information when it temporarily linked subscriber IDs with IP addresses. Thus, the complaint was well founded on the grounds that Bell was not open enough about their use of the technology, but not well founded insofar as customers consented to certain modes of data mediation in the terms of service, and the collection and usage of personal information was the minimum required to ensure network integrity and service quality. This is the most prominent evaluation of DPI by a privacy commissioner/data protection agency to date.

DPI and the Press

Bamford, James. (2008). *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America*. New York: Doubleday.

This text traces the NSA's integration of DPI appliances within key Internet infrastructure. Bamford first retells the September 11th terror attacks from the perspective of (failed) intelligence efforts. Ostensibly owing to these failures and combined with a



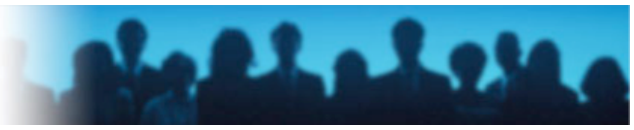
need to support both international and national security and intelligence operations, the NSA began integrating DPI appliances into communications hubs throughout America. Bamford provides a raft of empirical data on DPI deployments, identifying key landing stations for undersea data cables that the NSA, in cooperation with major American ISPs, intercepts, and Internet exchange and peering buildings where data is siphoned into secret rooms, processed, then shuttled to NSA data centers. He also describes the specific equipment that was deployed in AT&T controlled peering locations and their capabilities and provides detailed overviews of the sordid and controversial histories of two of the NSA's DPI vendors, Narus and Verint.

The book's fourth section traces the fallout of the NSA's surveillance program becoming public knowledge and sees Bamford argue that the Foreign Intelligence and Surveillance Act has failed to supervise secretive government surveillance. He concludes by noting that the NSA is accelerating its operations, expanding server farms, increasing computer power, hiring foreign language specialists, and preparing the equivalent of "first-strike" capabilities in case of a "cyber-war." DPI is far from the conclusion of the Agency's cyber-ambitions. If there is a key failing to this book, it is that Bamford's political attitudes seep throughout almost every page, forcing the reader to carefully evaluate the empirical data presented against potential biases in its documentation.

Anderson, Nate (2007). Deep packet inspection meets Net neutrality, CALEA. *Ars Technica*. Retrieved September 10, 2010 from http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars

In one of the earliest and most referenced popular articles on deep packet inspection, Anderson reports on the technical capacities, uses, and potential implications associated with networking technology. Carriers examine the payload, or content layer, of data packets that pass through ISPs' networks to determine what applications are transmitting and receiving data. Using application signatures (telltale identifiers based on the unique characteristics of applications' transmissions) particular traffic can be delayed, recorded, modified, or prioritized. Further, DPI permits more granular provision of Internet service; bandwidth caps can be diligently enforced and overage charges generated when partnering DPI equipment with account billing services, and particular services (e.g. online gaming) can be offered on a per-customer basis. DPI vendors maintain that service limitations can lower costs for end-users and that throttling (delaying) some application traffic produces a fairer network because it prevents any application from consuming more than its "fair share" of bandwidth.

Anderson recognizes that, if the last-mile market of Internet service is competitive, DPI might operate as an economic differentiator. He worries, however, that DPI equipment



could be inserted into backbone providers' networks and subsequently let them exert undue control over the data coursing across the Internet as a whole. Finally, DPI is often sold as being "CALEA Compliant," indicating that it conforms with US government surveillance laws. That many of these devices are sold internationally suggests that many of the routing devices deployed outside the US may conform to American, rather than local, Internet intercept and access policies.

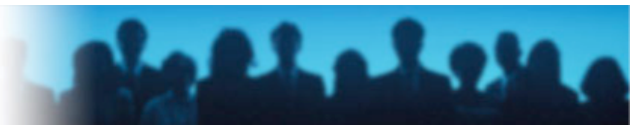
Additional Sources

Del Sesto Jr., Ronald W. & Frankel, Jon. (2008). How deep packet inspection changed the privacy debate. *Bingham (Law Firm)*. September 2008. Retrieved July 17, 2010 from http://www.bingham.com/Media.aspx?MediaId=7514

Online advertisers have relied upon contextual and behavioral advertising techniques to target ads to users. The FTC and Congress have been relatively inactive in addressing privacy concerns around these techniques, but this activity level might change with the integration of DPI into the advertising toolkit.

The analysis of whether and how DPI has impacted the American privacy debate revolves around NebuAd, a now-defunct advertising company that integrated DPI systems into ISPs networks to track and modify ISP customers' data traffic. As it became public knowledge that NebuAd was examining and modifying data traffic, largely because civil advocates exposed the practices, Congress held a series of hearings that evaluated the company and (more generally) the technologies that were driving its advertising model. The brief placement of DPI and behavioral tracking onto the federal agenda educated Congressional legislators about technical, privacy, and legal considerations surrounding the technology (an interest that has been sustained since this article's publication). Legislators criticized ISPs that worked with NebuAd on the basis that they provided insufficient notification; simply updating a many-thousand word privacy policy was recognized as insufficient notice. The authors refrain from suggesting how subsequent policy streams will take up DPI and, instead, conservatively state that DPI will remain a "controversial practice" that will "keep a variety of players in the online privacy debate engaged for years to come" (13). This has certainly been the case, with anti-tracking and pro-privacy legislation repeatedly making its way to the House floor since NebuAd's actions came to light.

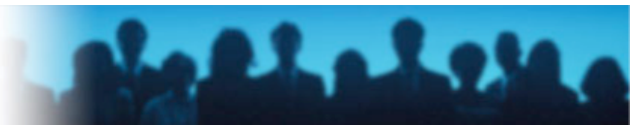
Mochalski, Klaus & Schulze, Hendrik. (2009). Deep packet inspection: Technology, applications, and net neutrality. *iPoque (DPI Vendor)*. Retrieved September 19, 2010 from http://www.ipoque.com/userfiles/file/DPI-Whitepaper.pdf



Mochalski' and Schulze's whitepaper distinguishes between DPI as a technology and its possible uses to modify social environments. While the technology can search for particular bits of information of interest, it cannot contextualize the information (i.e. peer-to-peer traffic may be identified, but the technology cannot make a normative judgment on the traffic), which the authors take to mean that the technology itself cannot violate someone's communicative privacy. The authors evaluate several of DPI's use-cases, including blocking encryption and tunneling systems that prevent lawful intercept of communications, blocking unregulated telephony applications, and blocking illegal content. They assert that any issues that arise from using the technology—censorship, maintaining monopolies, and so forth—are issues of *governance* instead of issues of the *technology*. Given the potentials of DPI equipment, Mochalski and Schulze assert that its uses should be regulated so that it can help regulate networks without threatening subscribers' privacy. Ultimately, society must be responsible for governing the uses of these devices; vendors should not be held accountable for merely providing a technical system that its owners can (or might) subsequently abuse.

Ramos, Anderson. (2009). Deep packet inspection technologies. In Harold F. Tipton and Micki Krause (eds.) *Information and Security Management Handbook (Sixth Edition), Volume 3*. New York: Auerbach Publications.

Ramos offers an overview of intrusion detection and prevention systems from the early 1990s to the present. Early Internet security relied on blocking/opening specific ports for application traffic, but this technique became ineffective as developers began channeling application traffic through known, typically open, network ports. Intrusion Detection Systems (IDS) were developed to prevent applications from exploiting open ports to route data but were of limited use in acting on suspicious application traffic. Deep packet inspection was, in part, a solution to the intrusion problem. It could operate inline with network traffic using one of two logics: pattern matching, which identified the application generating traffic and subsequently took action on it, or analyzing protocols to match them against whitelists or blacklists. The former approach required knowledge of the application's unique signature, to identify and take action upon it, whereas the latter requires only knowledge of permitted protocols (all others would be denied). While there is a set of technical issues with DPI, including its limited capacity to detect threats as effectively as previous network detection systems, Ramos takes pains to note that encryption largely undermines DPI's functionality. Specifically, "any type of encryption on the transport or network layer would compromise almost every basic functionality of DPI technologies, except for basic filtering" (2201). Given this issue and the number of protocols that by-default encrypt data traffic, Ramos suggests that security professionals should adopt intrusion protection controls that limit access to permitted protocols in the medium- to long-term.



Riley, Chris & Scott, Ben. (2009). Deep Packet Inspection: The End of the Internet As We Know It? *Free Press*. March 2009. Retrieved September 3, 2010 from http://www.freepress.net/node/49007

Today's Internet is guided by network neutrality, a principle that suggests that routers read packet headers and subsequently shuttle packets around the Internet on a best-effort basis. This idea is juxtaposed against a system where content is examined and data packets (de)prioritized based on packet contents. While DPI may have some benefits for network diagnostics and security, it is more substantively used to interfere with and modify data transmissions for advertising purposes, as well as to establish differential data traffic queues. Differential queuing threatens the development of new communication protocols because innovators cannot know if the ISP will (de)prioritize traffic associated with their protocol. The ISP, rather than simply being a conduit between clients, is assuming a significant role in how protocols are governed by adjudicating whether protocols receive priority in router queues.

Riley and Schott consider how the technology is marketed when evaluating its impact on the future of the Internet. According to vendors, DPI lets ISPs develop revenue streams based on the content customers want to access, in addition to selling the same customers Internet access. Further, inserting this technology into ISP infrastructure permits subsequent discrimination (e.g. against competing voice-over internet protocol providers), often on the grounds that discrimination limits the harm that developers' applications cause to the network. Such harms, however, are rarely substantiated. They authors worry that "bad uses" of DPI—discriminating against certain traffic, limiting service options—may undermine the neutrality the Internet has thrived on, ending the Internet's existence as an open platform for communication and innovation.