The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers?

by

Christopher Parsons
M.A, University of Guelph, 2007
B.A., University of Guelph, 2006

A Dissertation Submitted in Partial Fulfillment
of the Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Political Science

Supervisory Committee

The Politics of Deep Packet Inspection:
What Drives Surveillance by Internet Service Providers?

by

Christopher Parsons
M.A., University of Guelph, 2007
B.A., University of Guelph, 2006

Supervisory Committee

Dr. Colin J. Bennett, Political Science, University of Victoria
Supervisor

Dr. Arthur Kroker, Department of Political Science, University of Victoria
Departmental Member

Dr. Andrew Clement, Faculty of Information, University of Toronto
Outside Member

Abstract

Supervisory Committee
Dr. Colin J. Bennett, Department of Political Science
Supervisor
Dr. Arthur Kroker, Department of Political Science
Departmental Member
Dr. Andrew Clement, Faculty of Information, University of Toronto
Outside Member

Surveillance on the Internet today extends beyond collecting intelligence at the layer of the Web: major telecommunications companies use technologies to monitor, mediate, and modify data traffic in real time. Such companies functionally represent communicative bottlenecks through which online actions must pass before reaching the global Internet and are thus perfectly positioned to develop rich profiles of their subscribers and modify what they read, do, or say online. And some companies have sought to do just that. A key technology, deep packet inspection (DPI), facilitates such practices.

In the course of evaluating the practices, regulations, and politics that have driven DPI in Canada, the US, and UK it has become evident that the adoption of DPI tends to be dependent on socio-political and economic conditions. Simply put, market or governmental demand is often a prerequisite for the technology's adoption by ISPs. However, the existence of such demand is no indication of the success of such technologies; regulatory or political advocacy can lead to the restriction or ejection of particular DPI-related practices.

The dissertation proceeds by first outlining how DPI functions and then what has driven its adoption in Canada, the US, and UK. Three conceptual frameworks, path dependency, international governance, and domestic framing, are used to explain whether power structures embedded into technological systems themselves, international standards bodies, or domestic politics are principally responsible for the adoption or resistance to the technology in each nation. After exploring how DPI has arisen as an issue in the respective states I argue that though domestic conditions have principally driven DPI's adoption, and though the domestic methods of governing DPI and its associated practices have varied across cases, the outcomes of such governance are often quite similar. More broadly, I argue that while the technology and its associated practices

constitute surveillance and can infringe upon individuals' privacy, the debates around DPI must more expansively consider how DPI raises existential risks to deliberative democratic states. I conclude by offering some suggestions on defraying the risks DPI poses to such states.

Table of Contents

List of Figures

Abbreviations

ACLU	American Civil Liberties Union
ADSL	Asymmetric Digital Subscriber Line
AHSSPI	Aggregated High Speed Service Provider Interface
ARPA	Advanced Research Projects Agency
BAS	Broadband Aggregation Service
BBC	British Broadcasting Corporation
CAIP	Canadian Association of Internet Providers
CCDP	Communications Capabilities Development Programme
CCITT	Consultative Committee on International Telegraphy and Telephony
CDA	Communications Decency Act
CDB	Communications Data Bill
CDT	Center for Democracy and Technology
CERT	Computer Emergency Response Team
CIPPIC	Canadian Internet Policy and Public Interest Group
CLEC	Competitive Local Exchange Carrier
CO	Central Office
CRTC	Canadian Radio-television Telecommunications Commission
CSP	Communications Service Provider
DEA	Digital Economy Act
DMCA	Digital Millennium Copyright Act
DNSSEC	Domain Name System Security Extensions
DPC	Deep Packet Capture
DPI	Deep Packet Inspection
DSLAM	Digital Subscriber Line Access Multiplexer
EFF	Electronic Frontier Foundation
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission
FTC	Federal Trade Commission
FIPR	Foundation for Information Policy Research
FISA	Foreign Intelligence Surveillance Act
FPGA	Field-Programmable Gate Array
FTC	Federal Trade Commission
GAO	Government Accountability Office
GAS	Gateway Access Service
GCHQ	Government Communications Headquarters
IAB	Internet Architecture Board
ICO	Information Commissioners Office
IETF	Internet Engineering Task Force
ILEC	Incumbent Local Exchange Carrier
IMP	Internet Modernisation Programme
IoT	Internet of Things
IP	Internet Protocol
IPTV	Internet Protocol Television

IPv4	Internet Protocol version Four
IPv6	Internet Protocol version Six
ISO	International Standards Organization
ISP	Internet Service Provider
ISPA	Internet Service Provider Association
ITMP	Internet Traffic Management Proceeding
ITU	International Telecommunications Union
LSE	London School of Economics
MPAA	Movie Picture Association of America
MPI	Medium Packet Inspection
NDP	National Democratic Party
NSA	National Security Agency
OIX	Open Internet Exchange
OPC	Office of the Privacy Commissioner of Canada
OSI	Open Systems Interconnect
OTT	Over The Top
PIAC	Public Interest Advocacy Centre
PICS	Platform for Internet Content Selection
P2P	Peer to Peer
P3P	Platform for Privacy Preferences
RFC	Request for Comments
RIAA	Recording Industry Association of America
RIPA	Regulation of Investigatory Powers Act
SPI	Shallow Packet Inspection
TCP/IP	Transmission Control Protocol and Internet Protocol
TLS	Transport Layer Security
TOR	The Onion Router
US	United States
UK	United Kingdom
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WOW	Wide Open West

Acknowledgments

First, I would like to thank Dr. Omid Payrow Shabani for a conversation I had with him at the conclusion of my Masters degree, when he explained that it was possible to study deep packet inspection and its associated practices at a doctorate level. Prior to that conversation, I had seen my interests in digital technology as a hobby that was outside of academic interest; he put me on course to write this dissertation. I also want to thank him for giving me time to attend "The Revealed "I"" conference when I was his Master's student. That conference introduced me to many of my continuing colleagues and a world of academics studying technology, surveillance, and privacy issues.

My advisor, Dr. Colin Bennett, has provided tireless assistance in guiding me through the dissertation process. His intellectual, professional, and personal support for my work cannot be understated. Throughout our relationship, Colin has offered advice and assistance when I needed it, but left me alone enough to let me find my own ways. His willingness to introduce me to his colleagues inside and outside of academe have opened a host of doors that otherwise I would have never known about, let alone passed through. I owe an enormous amount to Colin for his commitment to supporting me as a young scholar.

Dr. Arthur Kroker and Marilouise Kroker have both made the University of Victoria a welcoming and challenging intellectual space, and I want to thank them for the kindness that they have provided and the intellectual rigour they have demanded. The opportunities that they have provided to me are appreciated, as is their support of my work over the past five years. They are exemplars of how scholars can, and should, work, collaborate, and support one another.

My scholarship, today, is very different in tone, aim, and intention than when I began my doctoral studies. Five individuals have been central to this change. Dr. Andrew Clement has offered excellent academic, and personal, counsel for navigating some of the projects related to my dissertation. His willingness to listen to, and provide advice about, some of the more stressful facets of my research has been incredibly generous. Pablo Ouziel's willingness to discuss the tactics of advocacy and how to put academic work into the public sphere has shaped how I understand and conduct civil advocacy. Christopher Soghoian stands as a model for how junior academics can contribute to formal literatures while simultaneously changing corporate and government practices. Jon Newton of P2PNet taught me how to punch above my weight, and provided me with a platform from which to speak. Finally, Adam Molar has been instrumental in thinking through the tactics of academic scholarship and how to simultaneously perform high calibre work while supporting members of civil society.

A great deal of my research and research network extends outside of academe. Mark Goldberg supported the earliest stages of my research by facilitating my attendance to the Canadian Telecommunications Summit, which helped me understand the issues facing Canadian ISPs while developing contacts that were subsequently helpful at later research stages. Others, such as Tamir Israel and Chris Prince, have been invaluable in honing my thinking around digital privacy and surveillance issues, while also supporting my work by suggesting ways to evade potential legal hazards. The same can be said for Micheal Vonn of the British Columbia Civil Liberties Association. Stuart Knetsch generously let me 'see' deep packet inspection appliances in operation, which helped me

appreciate their actual versus prospective capabilities. He also was an early critic of my analyses of the technology, which refined how I speak about and understand its operations. Kevin McArthur and Rob Wipond have been partners in opposing onerous government surveillance, as well as excellent friends who have always been willing to listen and help me to work through strategies and tactics around my scholarship and advocacy.

Throughout my Ph.D I have worked with earnest and dedicated journalists who have taken up privacy issues. I appreciate the work that they are doing – it's often hard to 'sell' privacy stories to editors – and thank those who took the time to teach me how to present information to the media.

My interview subjects are not named in my dissertation, but I want to thank them all. Corporate executives, harried civil advocates, hardworking journalists, and government policy analysts all kindly gave their time for interviews, and those interviews have enhanced my understanding of the politics of deep packet inspection.

A host of organizations have supported my research. The Office of the Privacy Commissioner of Canada provided funding through its contributions program that jumpstarted my Canadian research into deep packet inspection. The Office has also, subsequently, supported some of my analysis of lawful access as it pertains to online communications platforms. Dr. Ann Cavoukian (Information and Privacy Commissioner of Ontario) and Elizabeth Denham (Information and Privacy Commission of British Columbia) have been supportive of my research program as well, giving me opportunities to discuss pressing privacy issues with members of their Offices. A set of civil society groups, including the British Columbia Civil Liberties Association, British Columbia Freedom of Information Association, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, Electronic Frontier Foundation, Privacy International, and Open Media have also supported my work; some have financially supported it, others have publicized it, and yet others have offered key resources to deepen my understanding of online privacy and surveillance issues.

My dissertation has been written in a series of academic bodies. The Department of Political Science at the University of Victoria generously provided first-rate office space, where much of my early writing and research took place. The Faculty of Information at the University of Toronto kindly found space for me when I visited for a month; it was there that I completed and presented on the second chapter of my dissertation. The final leg of my writing has occurred in the Centre for Global Studies; the Centre has provided an incredibly hospitable and intellectually stimulating environment. The fellows, staff, and associates have been truly delightful to work beside.

Finally, I want to thank two of my family members in particular. Joyce Parsons has been a tireless editor of my work; she has identified errors in my arguments, strengthened my prose, and indicated where additional lines of analysis could be performed. At this point, she is probably amongst Canada's leading experts on Internet surveillance and deep packet inspection. Luciana Daghum has been with me throughout the doctorate; I've often been overcome by foul moods while writing and researching, but she has remained beside me and never let me quit, no matter how badly I've wanted to. Her optimism has been the life preserver I've grasped after, and always found, in the many darker days of the dissertating process.

Chapter 1: Introduction

Network surveillance practices are becoming increasingly common aspects of daily life. Internet service providers monitor certain application traffic and block or delay its delivery.[1] Major advertising companies monitor users' movements across the Web to customize advertising for them.[2] Chat services scan messages to evaluate whether they contain links to malware or language that is deemed impermissible by the service provider.[3] Governments are increasingly invested in passing legislation to monitor the Internet for persons that are of interest to authorities'.[4]

Surveillance on the Internet today, however, extends beyond collecting intelligence at the service layer of the Web: today, major telecommunications companies, such as Internet Service Providers (ISPs) use technologies to monitor, mediate, and modify data traffic in real time. These companies are privy to all of our digital movements, transmissions, and conversations and functionally represent communicative bottlenecks through which our online actions must pass before being transmitted to the global Internet. These companies are perfectly positioned to develop rich profiles of their subscribers and modify what they read, do, or say online. And some companies have sought to do just that. A key technology, deep packet inspection, facilitates these practices.

Not all companies have engaged in total network surveillance, nor have all companies engaged in the *same kinds* of surveillance. Indeed, the potentials of network-level surveillance are often distinct from the realities of corporate and government practices. The motivations that are perceived as driving these network practices are *also* sometimes distinct from the actual drivers. In this dissertation I render transparent the politics that have driven the uses of deep packet inspection in Canada, the United States, and United Kingdom. As such, this work shines a light into the murk of technical

---

[1] Nate Anderson, "Canada: ISP traffic shaping should only be "last resort"," *Ars Technica*, October 21, 2009, accessed September 9, 2013, http://arstechnica.com/tech-policy/2009/10/canada-isp-traffic-shaping-should-only-be-last-resort/.

[2] Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising," *Office of the Privacy Commissioner of Canada*, June 6, 2012, accessed September 9, 2013, http://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp.

[3] Ryan Singel, "New Facebook Messaging Continues to Block Some Links," *Wired*, November 18, 2010, accessed September 9, 2013, http://www.wired.com/business/2010/11/facebook-link-blocking/.

[4] Ron Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: McClelland & Stewart, 2013).

demands, business objectives, national security, and regulatory politics to ascertain what is, and is not, behind the adoption and rejection of network surveillance facilitated by deep packet inspection.

Deep Packet Inspection

Internet traffic is made up of packets of data that can generally be understood as possessing two key components: header information and payload information. Header information provides routing information so that Internet communications can reach their destination(s), whereas payload information contains the content of what is being transmitted. This latter information includes the application generating or receiving the data transmission (e.g. Thunderbird or Outlook or Apple Mail) as well as the content of what is being communicated (e.g. the words of the email and to whom it is addressed). The ability to seamlessly act on both header and payload information, in real time, provides a significant degree of control over communications: a party capable of acting on such information could change what is said, when it is said, and to whom it is said. Network controllers, such as Internet service providers, have increasingly deployed network technologies that provide the ability to massively monitor data packets. This technology is known as deep packet inspection.

Deep packet inspection (DPI) builds on earlier networking capabilities that afforded more limited insight into the contents of what Internet subscribers were receiving and transmitting. DPI appliances can be programmed to analyze and act on header and payload information in real time, often in such a way that it is not apparent to subscribers that their network operator is monitoring, mediating, or modifying data transmissions. The capacity to act on data transmissions in such a totalizing way makes the technology capable of adapting to a series of different use cases and associated practices. These appliances can be used to moderate the flow of certain kinds of traffic, such as those linked with voice over Internet protocol or peer-to-peer transmissions, or they can intentionally identify and block traffic linking those kinds of services.[5] These kinds of practices could be performed to reduce the overall amount of data traffic flowing across a network, perhaps when a router cannot forward all the data packets it is receiving

[5] Office of the Privacy Commissioner of Canada, "What is DPI?", *Office of the Privacy Commissioner of Canada*, April 2009.

to adjoining routers, or they could be used to discriminate against competitors' business offerings while enhancing the reputation of a network operators' own services, which are not subject to such practices.

Network operators can also intentionally 'close' transmissions between applications by injecting commands that inform applications on peoples' computers that the transmission has failed, regardless of whether this is actually the case.[6] In an associated vein, operators can modify data traffic such that specialized tracking information is embedded in packets – changing the payloads themselves – to subsequently deliver highly targeted advertisements.[7] The close reading of packet payloads could also be used to identify and, potentially, stymie the dissemination of copyright infringing files.

The aforementioned uses are predominantly *private* uses of the technology to accomplish the goals of private actors. However, deep packet inspection could also be used for state surveillance or security policies: appliances could be configured to monitor for certain kinds of online communications, certain contents of communication, or appliances could be used as part of a broad state surveillance assemblage to profile citizens and resident aliens.[8] Given the common perception that 'once it's built, it's hard to remove' any kind of technical infrastructure, the stakes that are perceived as being linked with deep packet inspection run high amongst the various parties who are interested in the technology and its associated practices.

Interested Parties

Given the potential uses of deep packet inspection appliances, civil society advocates, government institutions, and groups that conduct their business over the Internet have sounded a host of alarms. Internet Service Providers (ISPs) and government regulators

---

[6] Robb Topolski ("Funchords"), "Comcast is using Sandvine to manage P2P Connections," *DSL Reports Forum*, May 12, 2007, last accessed September 7, 2013, http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections.

[7] Andreas Kuhn and Milton Mueller, "Profiling the Profilers: Deep Packet Inspection for Behavioural Advertising in Europe and the United States," *SSRN*, September 1, 2012, accessed March 1, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181.

[8] William Binney, quoted in Ms. Smith, "HOPE 9: Whistleblower Binney says the NSA has dossiers on nearly every US citizen," *Network World,* July 15, 2012, accessed March 8, 2013, https://www.networkworld.com/community/blog/hope-9-whistleblower-binney-says-nsa-has-dossiers-nearly-every-us-citizen.

have often sought to calm worries that the technology could be used for mass surveillance. In other instances, however, government bodies have advanced the ideas that the technology could potentially be used, or is already being used, to enhance state security or foreign intelligence practices.[9]

Given their centrality to Internet communications, ISPs have become the linchpin in all major debates concerning the technology. These companies have also expressed their own interests in practices linked to packet inspection: it could help them reduce data congestion at their routers, but, at the same time, it could be used to delay making capital investments in networking infrastructure.[10] The technology could also be used to enhance revenue streams by tracking subscribers' online behaviors and serving those same people online advertisements for products and services that they might be most interested in. Finally, the technology could help secure deals with music and video producers by monitoring for, and interdicting, data transmissions carrying copyright infringing files.[11] Vendor partners, who stand to benefit from sales and maintenance of deep packet inspection appliances, have often supported ISPs.

While one set of business interests might advocate for the adoption of deep packet inspection, other companies and organizations have fought against its deployment. Such critical companies often produce content for the Internet, or they deliver other parties' content using online distribution mechanisms, and are thus competing against ISPs' content offerings. These competitors warn that Internet service providers retain an interest in discriminating against their competitors and that, if such discrimination manifests itself, novel business models and entrepreneurial firms may fail to take hold in the market.

Similar warnings have been taken up by civil and consumer rights advocates. Such advocates warn that deep packet inspection is inherently privacy-invasive, insofar as it depends on analyzing and acting against the contents of communications. Such surveillance practices are characterized as being normatively inappropriate and often as running counter to national laws, which forbid intercepting citizens' communications

---

[9] Interview with senior UK telecommunications consultant, September 18, 2012.
[10] Interview with Canadian telecommunications executive, January 31, 2012.
[11] Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the Network: Using DPI for Copyright Enforcement," *Surveillance and Society* 9(4) (2012)

without a warrant. [12] These advocates often have strong reservations about the very existence, let alone use, of deep packet inspection but tend not to oppose the technology itself. Instead, they focus on the technology's associated practices.

Domestic state institutions have often been deeply influential concerning which DPI related practices are or are not permitted. Government regulatory forums have exerted differing levels of power and influence over how the technology can be used, and it is common for different government institutions to take interest in different practices. Government institutions have not been just adjudicators of non-state actors' conflicts; they are often the forces that have driven or opposed specific practices. In some instances, these institutions have identified deep packet inspection practices as one (amongst many) means of extending or enhancing their power: my analysis of deep packet inspection has revealed that government institutions have often driven the agenda concerning how the technology can monitor and modify citizens' and resident aliens' data traffic.

Outside of purely domestic parties, members of international governance organizations such at the International Telecommunications Union and World Wide Web Consortium can potentially play a role in the technology's permitted practices. Heralded alternately as impotent and devastatingly important,[13] international standards organizations are seen as potentially playing a role in how deep packet inspection can and cannot be used. While the digital code that lets people communicate enforces certain requirements – it sets down a 'law' concerning the content and format of communications[14] – standards bodies are sometimes recognized as non-governmental legislative assemblies of the digital law by virtue of standards-setting activities.[15] Hence the positions, standards, and actions that these bodies assume can both reflect and

---

[12] Nicholas Bohm, "The Phorm "Webwise" System – a Legal Analysis," *FIPR*, April 23, 2008, accessed May 10, 2013, http://www.fipr.org/080423phormlegal.pdf.

[13] Milton Mueller, "ITU Phobia: Why WCIT Was Derailed," *Internet Governance Project*, December 18, 2012, accessed September 8, 2013, http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

[14] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books).

[15] Harry Hochheiser, "Indirect Threats to Freedom and Privacy: Governance of the Internet and the WWW," *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*, (2000).

prospectively influence how domestic actors justify or frame their own favored uses of deep packet inspection.

All of these parties are often uncloaked or discussed by the trade presses and the mass media. News organizations recognize that mass surveillance technologies are both newsworthy and are sufficiently 'bloody' stories that they attract readership. As journalists cover the various practices and actors linked with the technology, other parties emerge from the woodwork to engage in policy arenas on the basis that deep packet inspection might be an issue for them. The press has played a crucial role in spreading information about the potentials of the technology, influenced the roles that various parties have assumed, and swayed the successes and failures that parties have had in advancing their interests.

The Sites of Study

Wherever deep packet inspection has been deployed, the aforementioned cast of parties tend to be found. As such, most countries in the world could function as sites of study given the technology's widespread adoption. This dissertation specifically focuses on Canada, the United States, and the United Kingdom because of their common language, their longstanding memberships in key international standards bodies, their leading adoption of Internet services, and their mature regulatory organizations.

With a common language, the various parties interested in deep packet inspection can, at least potentially, communicate with one another without language barriers preventing such discourse. As a result, individuals can develop interpersonal relationships and share information across borders; the networks that can form are not unduly stymied by language differences. Moreover, a similar written literacy means that parties can read about what is happening in other English speaking jurisdictions and ascertain how what is happening abroad might parallel their domestic situation. In effect, a similar language reduces the friction of developing international policy networks that can learn from, and share with, parties in other states.

If standards bodies are the prospective legislative bodies of digital 'law', then the members of those bodies play a key role in advocating for and legitimizing such 'laws'. The countries under study are long-standing members of some state-dominated bodies,

and parties within these states have had roughly equal (temporal) opportunities to join non-governmental driven institutions. As a result, members of these states could be – although are not necessarily – similarly represented in international standards bodies. If these bodies are truly significant, then equalizing the (relative) power differentials between case sites permits a more equitable evaluation of how domestic parties have affected, and been affected by, international standards organizations.

Canada, the United States, and United Kingdom all saw early adoption of Internet technologies. Even while state institutions may have been slow to adopt Internet services, some non-governmental actors saw potentials linked to the Internet. ISPs have not been the sole or even the primary parties that have recognized such potentials: members of civil society, small businesses, and non-governmental organizations all have seen how the Internet could enhance or undermine their own interests. Because each of these states saw the early adoption of the technology, a similar temporal opportunity existed for advocacy groups to spawn - advocating for how Internet services can, should, and should not be affected by the gatekeepers of the Internet. As a result, there have been relatively similar conditions for business, non-profit, and government institutions to develop an interest in Internet communications and, consequently, react when private or public organizations advocate for or against uses of deep packet inspection that might affect communications flows.

In tandem with the early adoption of Internet services in these countries, regulators have had time to learn about the Internet. Canada, the United States, and the United Kingdom have regulators that are, at this point, versed in regulating online behaviors. This is not to say that regulators are infallible, omniscient, or omnipotent, but that they have a history of regulatory decisions that potentially help guide their decisions concerning how deep packet inspection can, should, and should not be used. Moreover, the maturity of these institutions means that their members have had ample opportunities to develop cross-border and international relations with other regulators and international bodies responsible for overseeing the appropriate transmission of data throughout national and cross-national data networks.

At the same time, there are some key and significant differences between these three cases. First, each nation has a different means of protecting residents' privacy or

personal data from inappropriate uses; whereas Canada's federal Office of the Privacy Commissioner is appointed by Parliament and is responsible for investigating breaches of federal privacy law, the Office acts in an ombudsperson. This is contrasted against the UK's Information Commissioner, which is charged with investigating complaints as a regulator, and the FTC, which investigates and levies fines against organizations found to make deceptive privacy claims. Moreover, whereas as the former two states possess comprehensive privacy laws this is not the case in the United States, which has a patchwork of federal and privacy laws that establish a mosaic of data protection and privacy regulations. This patchwork does not necessarily mean that there are *weaker* laws in the US, but that the protection of personal information and data comes from a more diverse set of federal and state laws and, thus, there is a more varied domain of law that could be used to restrict DPI-based practices.

In addition to divergent means of protecting privacy, the states under study have significantly different telecommunications ecosystems. In Canada, dominant ISPs must make their infrastructure available to competitors at a regulated cost by CRTC order, whereas in the UK there is a division between 'wholesale' and 'retail' telephone-based broadband networks, and in the US there is an entrenched (and politically influential) oligarchy of telecommunications companies. This means that ISPs hold varying economic stakes in controlling traffic that is at least partially dependent on their telecommunications regulatory framework. Moreover, while each nation possesses telecommunications regulators they are not of equal influence or power: the relative impotence of the American government's Federal Communications Commission, demonstrated in their reduced regulatory power following legal challenges brought by Comcast,[16] compared to Canadian and UK regulators, could affect the regulatory debates concerning how ISPs deploy DPI.

Beyond these legal and infrastructure and business differences, the states under study have exhibited differing political interests in DPI: the technology and its associated practices has only minimally arisen on the Canadian political agenda, whereas in both the UK and US there has been some degree of interest in the technology by legislative and

---

[16] Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press, 2013).

executive branches of government. In aggregate, while there are sufficient commonalities between cases to enable comparisons across states, the differences between these cases means that national particularities could lead to variations in how DPI-related issues are taken up as a result of these states' respective privacy, telecommunications, or political conditions.

Methodology

Methodologically, this dissertation has sought to understand holistically the politics behind what is driving deep packet inspection. This comparative project is inductive and progressed along different levels of analysis. In the first line of analysis I engaged in a detailed technical analysis of deep packet inspection on the basis that little had been written about DPI as a technology itself; as such, I had to provide an analytic account of what the technology does and the practices to which it could be linked. This analytic work was supplemented by a series of theoretical frameworks that provided a means of examining the technology and explaining its practices in the case studies. In the second line of analysis I provided a descriptive account of how the technology is, has been, or is planned to be, deployed in Canada, the US, and the UK. This second stage of the research project established the data that was needed to derive lessons and theoretical insights in the third, and final, stage of the dissertation. This third stage identified what is actually driving the technology, whether there were commonalities or variations in the drivers, and the broader significance of DPI for theories of surveillance and democratic governance

To engage in my analysis of DPI I adopted a series of techniques to understand both what has been publicly stated about the technology's uses as well as to discover previously unexplored empirical data. Document analysis and expert-level interviews were complemented by media reports and other secondary documents to ascertain what is driving the politics of deep packet inspection in Canada, the United States, and the United Kingdom. Documentary analyses relied on reviewing publicly available documents that were in regulatory arenas, on corporate and private websites, and, in some cases, documents that had been leaked to whistle-blowing websites. Core or significant

statements and issues were identified in those documents and used to explain how and why actors advanced their interests concerning packet inspection practices.

Primary source document analysis was supplemented by elite-level interviews. Interviews were either anonymous or off the record; in the former cases, I refrain from naming even the specific organizations for which interviewees work. Interviews used a common set of semi-structured questions; interviewees were encouraged to identify issues or topics that were not previously included as questions, and they were invited to identify other actors with whom I should speak. Experts were drawn from the ranks of telecommunications executives, consumer and civil advocates, government regulators, and journalists. Interviews were recorded and lasted between 30-90 minutes. Interviewees approved direct quotations prior their to use in this dissertation.

Secondary-sourced documents and reports about the politics of deep packet inspection were used to flesh out and explain in more depth what was driving the adoption or opposition of particular practices. Media reports were relied on for quotations that gave insight into parties' intentions for the technology, as well as for factual information that was not easily accessible in primary source documents. Other secondary source documents, such as academic articles and books, as well as books oriented towards public audiences, provided additional empirical data and were used to understand parties' motivations for driving or opposing packet inspection practices.

Using these data sources, I explored the politics driving deep packet inspection across the sites of study. When combined with the three-stage analysis (descriptive, comparative, theoretical) my methodological approach let me understand what groups said about DPI while offering the tools to evaluate their statements. The result of these methodological choices was that I could evaluate differences and commonalities across cases, while situating them against the broader significance of how online surveillance is conducted in democratic countries, and how such surveillance could affect democratic governance practices.

Outline of Dissertation

This dissertation is divided into three parts. The first three chapters provide the foundation from which we can evaluate how and why deep packet inspection is adopted.

Chapter Two offers a technical discussion of why deep packet inspection is part of an ongoing lineage of packet inspection systems and explains in some depth how it could be used in our sites of study. Chapter Three offers a set of frameworks against which we can evaluate why deep packet inspection is being adopted and used, and what might explain any cross-national differences and similarities. Specifically, this chapter suggests that path determinacy, international relations and governance, or policy framing theories could explain what is driving the politics of deep packet inspection.

The second part of the dissertation analyzes the empirical cases. Chapters Four, Five, and Six outline how deep packet inspection is framed by actors in Canada, the United States, and United Kingdom, respectively. Each chapter adopts a common structure and explores common issues in order to understand whether some issues are more significant than others in the different states, and to explore how parties sought to frame practices linked to deep packet inspection in each nation. Each chapter sees a common series of policy communities involve themselves in the debates concerning the technology, though their effectiveness in advancing their interests varies. By the conclusion of Chapter Six, the stage will have been set to establish commonalities and differences behind what is driving, or has driven, the adoption or rejection of practices linked to deep packet inspection.

The final part of the dissertation includes Chapters Seven and Eight, which develop lessons and provide theoretical insights into the nature of Internet-based surveillance. Chapter Seven explores the politics of deep packet inspection by way of comparing the experiences in Canada, the United States, and United Kingdom. It draws general conclusions about what is, and is not, driving the technology's adoption and discusses the importance of institutional cultures and the vibrancy of civil advocacy efforts to understand how technical systems such as deep packet inspection are taken up by government institutions. I argue that DPI raises existential questions of communications control for many actors, and that despite variances in how DPI-related practices have been taken up in each nation there has been common conclusions to when, and how, the technology can be used. Chapter Eight concludes the dissertation by considering the broader normative significance of inserting deep packet inspection appliances throughout Internet networks. Questions of controlling communications,

monitoring communications, and the privacy implications of examining data transmissions were raised across case studies; while the literatures of surveillance and privacy provide some ways of theoretically considering the broader democratic implications of DPI controlling communications flows, each literature suffers from theoretical deficiencies. As a result, I suggest that the concepts of surveillance and privacy provide necessary, but insufficient, grounds to critique DPI-based practices; what is needed instead is a democratic theory that avoid the flaws of surveillance and privacy literatures while also focusing on the importance of uncoerced communications in generating political legitimacy. On this basis, I turn to deliberative democratic theory to critique how DPI is used on normative grounds while also showing how this particular democratic theory provides useful policy recommendations capable of mediating DPI's most threatening characteristics. The result is to understand not just how DPI is framed in institutional arenas in the course of policy framing, but to grasp the broader implications of what DPI might mean for contemporary democracies.

Chapter 2: Deep Packet Inspection and Its Predecessors

The earliest social choices and administrative decisions guiding the Internet's growth emphasized packet delivery over infrastructural or data security.[17] These early choices have led to an Internet that is fundamentally predicated on trust and radical vulnerability, insofar as individuals must trust that their data will arrive at its destination without interference. The 'default setting' of Internet communications is hope that no other agent will take advantage of the fact that most peoples' communications are transmitted throughout the Internet in easily read plaintext. Methods that secure this vulnerable data traffic, such as encryption, obfuscation, and forensic real-time packet analysis, are effectively a series of kludges that are bolted onto an architecture designed primarily to ensure packet delivery. Whereas packet inspection technologies initially functioned for diagnostic purposes, they are now being repositioned to 'secure' the Internet, and society more generally, by taking advantage of the Internet's vulnerabilities to monitor, mediate, and modify data traffic. Such inspection capabilities reorient the potentialities of the digital medium by establishing new modes of influencing communications and data transfers, thus affecting the character of messages on the Internet. Whereas the early Internet could be characterized as one of trusting the messenger, today the routing infrastructure responsible for transferring messages may have been secretly inspected, recorded, or modified messages before passing them towards their destination; today the Internet is a less trustworthy infrastructure.

This chapter traces a lineage of contemporary packet inspection systems that monitor data traffic flowing across the Internet in real time. After discussing how shallow, medium, and deep packet inspection systems function, I outline the significance of this technology's most recent iteration, deep packet inspection, and how it could be used to fulfill technical, economic, and political goals. Achieving these goals, however, is not accomplished using a uniform piece of technology: DPI appliances are often specifically configured for discrete tasks and the range(s) of acceptable tasks are shaped by social regulation. Given the importance of Internet-based communications to every

---

[17] Susan Landau, *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies* (The MIT Press, 2011), 39.

facet of Western society, from personal communications, to economic, cultural, and political exchanges, deep packet inspection must not just be evaluated in the abstract but with attention towards how society shapes its deployment and how it could be used to shape society.

A Chronology of Data Packet Inspection

Network administrators initially logged some network activity to identify and resolve network irregularities when ARPANET, the predecessor to the public Internet, was under development.[18] Logging let administrators determine if packets were being delivered and whether network nodes were functioning normally. At this point, security was an afterthought, at best, given that the few people using the network were relatively savvy users. Before the first piece of software that intentionally exploited the network was released, ARPANET and its accompanying workstations operated in a kind of 'network of Eden.'

For ARPANET, the poison apple was the Morris worm. Whereas viruses tend to be attached to files, worms are typically autonomous programs that burrow into computers and simply spread. Their primary function is to be self-replicating, with other functionality, such as viral attack code, often being appended to them. Morris compromised computers connected to ARPANET without damaging core system files, instead slowing down computers until they had to be rebooted to restore their usability.[19] The worm spread to hundreds of computers and led to significant losses to available computing time. In Morris' aftermath, the security of the network became a more prominent concern in the minds of researchers and any general users who understood what had happened.

To mitigate or avoid subsequent disseminations of malware (harmful software intended to impair or act contrary to the computer owners' intentions or expectations), "computer science departments around the world tried to delineate the difference between

---

[18] Katie Hafner, *Where Wizards Stay Up Late: The Origins Of The Internet* (Simon & Schuster, 1998), 161-165.

[19] While there are claims that thousands of computers were infected by the worm, no one can be certain of such numbers. Paul Graham has stated that he was present when a 'guestimate' of 6,000 infected computers was arrived at. This estimate was based on the assumption that about 60,000 computers were attached to the network, and roughly 10 percent assumed compromised. Paul Graham, "The Submarine," *Paul G*, accessed March 22, 2013, http://www.paulgraham.com/submarine.html#f4n.

appropriate and inappropriate computer and network usage, and many tried to define an ethical basis for the distinctions."[20] The diagnosis of the Morris worm also provoked extended discussion about computer ethics by the Internet Engineering Task Force (IETF),[21] the Internet Activities Board,[22] National Science Foundation,[23] Computer Professionals for Social Responsibility,[24] as well as in academic, professional, and popular circles.[25] Further, the Computer Emergency Response Team (CERT), which documents computer problems and vendor solutions, was formed. Computer firewalls also received additional attention. While firewalls, which are designed to permit or deny transmissions of data into networks based on rules established by a network administrator, had been in development before the Morris worm, in the aftermath of the worm and the shift towards a broader public user base, firewalls were being routinely deployed by 1994-5.[26]

Data Packets 101

Firewalls are effectively packet analysis systems, and are configured to "reject, allow, or redirect specific types of traffic addressed to specific services and are (not surprisingly) used to limit access to certain functions and resources for all traffic traveling across a device."[27] They have evolved in three general waves since the mid-90s: shallow packet, medium packet, and deep packet inspection.

While early packet analysis systems merely examined information derived from data packets' headers, such systems now examine both the header and the payload. The header includes the recipient's Internet Protocol (IP) address, a number that is used to

---

[20] Hilarie Orman, "The Morris Worm: A Fifteen-year Perspective," *Security and Privacy, IEEE* 1(5) (2003), 40.
[21] J.K. Reynolds, "RFC 1135: Helminthiasis of the Internet," *IETF Network Working Group*, 1989, accessed March 25, 2013, https://tools.ietf.org/html/rfc1135.
[22] Internet Activities Board, "Ethics and the Internet," *Communications of the ACM 32(6)* (1989).
[23] National Science Foundation, "NSF Poses Code of Networking Ethics," *Communications of the ACM 32(6)* (1989).
[24] Computer Professionals for Social Responsibility, "CPSR Statement on the Computer Virus," *Communications of the ACM 32(6)* (1989).
[25] See Section 9: Bibliography of J. K. Reynolds, "RFC 1135: The Helminthiasis of the Internet," IETF Network Working Group, December 1989, accessed March 21, 2013, http://tools.ietf.org/html/rfc1135.
[26] Hilarie Orman, "The Morris worm: a fifteen-year perspective," *Security and Privacy, IEEE* 1(5) (2003), 35-43.
[27] Michael Zalewski, *Silence on the Wire: a Field Guide to Passive Reconnaissance and Indirect Attacks* (San Francisco: No Starch Press, 2005), 174.

reassemble packets in the correct order when recompiling the messages and to deliver packets to their destination(s). At a more fine-grained 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 header and payload are derived from the Open

Level	OSI Model	Payload/Header Division
7	Application Layer	Payload
6	Presentation Layer	
5	Session Layer	
4	Transport Layer	
3	Network Layer	Header
2	Data Link Layer	
1	Physical Layer	

Figure 1: The OSI Packet Model

Systems Interconnect (OSI) packet 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, though it was abandoned for practical networking activities in favor of the Transmission Control Protocol and Internet Protocol Suite (TCP/IP). OSI's most significant contribution to network development efforts has been to force "protocol designers to be more conscious of how the behavior of each protocol would affect the entire system."[28] OSI stands in contrast to TCP/IP's key contribution, which was to create a fungible system that maximized interoperability by minimizing system interfaces (IP) and checking for packet delivery and network congestion (TCP). TCP/IP's other key contribution was that it ensured that the ends of the network, as opposed to the core, would govern the flow of data packets. In a TCP/IP network, client computers are primarily responsible for

[28] Jennifer Abbate, *Inventing the Internet* (Cambridge, Mass.: The MIT Press, 1999), 177.

controlling the flow of packets and, as such, limit network owners' control over what, why, and how packets course across the Internet.[29]

When sending a packet of data, the Application Layer interacts with the piece of software that is making a data request, such as the email client, web browser, instant messaging software and so on. 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 stack. When the browser receives a response from the server that hosts the requested page on the Internet, 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 encrypts and compresses data. In the case of a webpage, this stage is where the data request is identified as asking for an HTML file. The fifth layer, the Session Layer, creates, manages, and ends communications within a session 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 connection between the sender(s) and recipient(s) of packets. In terms of a web browser, this layer establishes the connection between the computer requesting data and the server that is hosting it. It also ensures that packets are properly ordered so that the aggregate data they contain are meaningfully (re)arranged when the packets arrive at their destination. 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

[29] Jennifer Abbate, *Inventing the Internet* (Cambridge, Mass.: The MIT Press, 1999), 194.

assumes that role. The Data Link Layer formats the packet so that it can be sent along the medium being used to transmit the packet from its point of origin to its destination. As an example, this layer can prepare packets 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 wireline networks, and then back to a wireless format when being received by a colleague in their office whose 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.

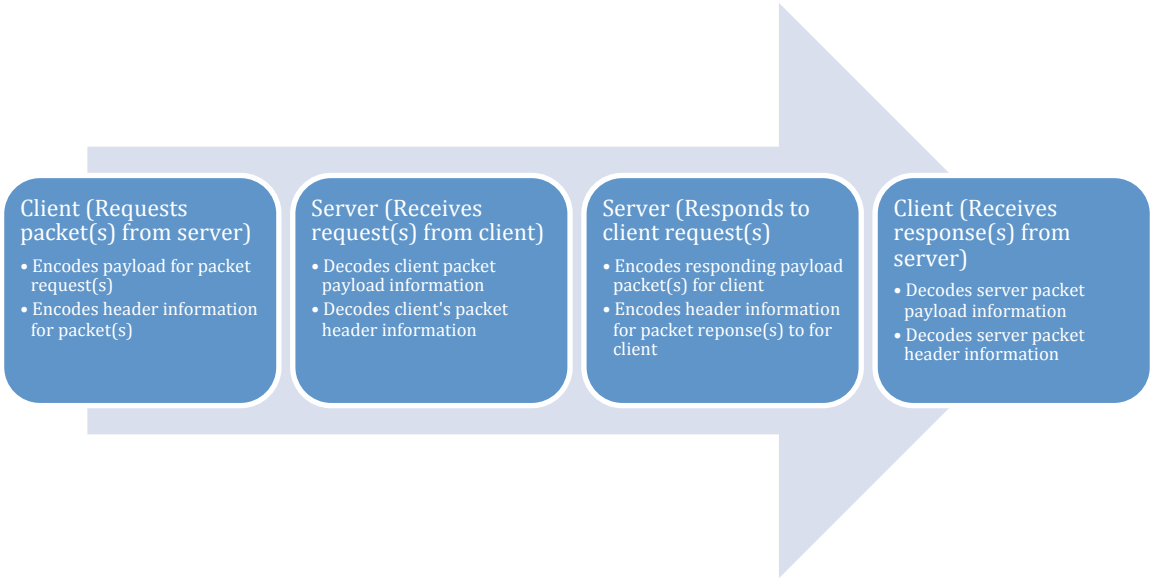


Figure 2: Client-Server Data Transaction

Packets are typically 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 receives and decodes the packet to provide the application with the requested information. Key to this flow diagram is that there is often a piece of equipment or software that conducts packet analysis between the client and server; for our purposes, this intermediary is packet inspection software or equipment.

Shallow Packet Inspection

Shallow Packet Inspection (SPI) technologies depend on (relatively) simplistic firewalls and were used for early consumer firewalls. These technologies limit user-specified content from 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 against which data are evaluated, whereas in others, network administrators are responsible for creating and updating the rule set. Specifically, these firewalls focus on the source and destination IP address that the packet is trying to access and the packet's port address. If the packet's header information – either an IP address, a port number, or a combination of the two[30] – is on the blacklist, then 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.[31] More advanced forms of SPI capture logs of incoming and outgoing source/destination information so that a systems administrator can later review the aggregate header information to adjust, or create, blacklist rule sets.

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 the packets to be reassembled into a format that the receiving application can understand. SPI cannot read the session, presentation, or applications layers of a packet; it cannot peer into a packet's payload and survey the 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

---

[30] Thomas Porter, "The Perils of Deep Packet Inspection," Symantec Corporation, last modified October 19, 2010, accessed March 21, 2013, http://www.symantec.com/connect/articles/perils-deep-packet-inspection.

[31] 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.

proxies can examine packet header information against their loaded parse-list[32] and are often used by businesses to monitor for specific application flows. Parsing involves structuring data as "a linear representation in accordance with a given grammar."[33] While finite languages can provide infinite numbers of sentences/linear representations, a parse list holds a set of particular representations and, upon identifying them, takes specified action against them. In effect, this means that MPI devices bridge connections between computers on a network and the Internet at large, and they are configured to look for very particular data traffic and take preordained actions towards it.

More specifically, in the case of MPI devices, this activity entails examining packet headers and a small amount of the payload, which together can assume an infinite number of potential representations, for particular representations derived from specific header and payload combinations. Importantly, parse-lists are subtler than blacklists. 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. Further, parse-lists can easily be updated to account for new linear representations that network administrators want to remain aware of, or modify existing representation-sets to mitigate false-positives. As such, MPI constitutes an evolution of packet awareness technologies, insofar as this means of packet inspection can more comprehensively 'read' the packet and take a broader range of actions against packets that fall within their parse-list definitions.

Application proxies intercept data connections and subsequently initiate new connections between the proxy and either the client on the network (receiving data from the Internet) or between the proxy and data's destination on the Internet (when transmitting data to the Internet).[34] These proxy devices 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

---

[32] 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.

[33] Dick Gune and Ceriel J.H. Jacobs, *Parsing Techniques: A Practical Guide* (West Sussex: Ellis Horwood Limited, 1990), 1.

[34] Michael Zalewski, *Silence on the Wire: a Field Guide to Passive Reconnaissance and Indirect Attacks* (San Francisco: No Starch Press, 2005), 146.

applied to all data streaming through the network. Figure three offers a visual representation of how this placement might appear in a network. Placing devices inline 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 thus provides network administrators with the ability to force client computers to authenticate to the proxy device before they can receive packets from beyond the administrator's network.

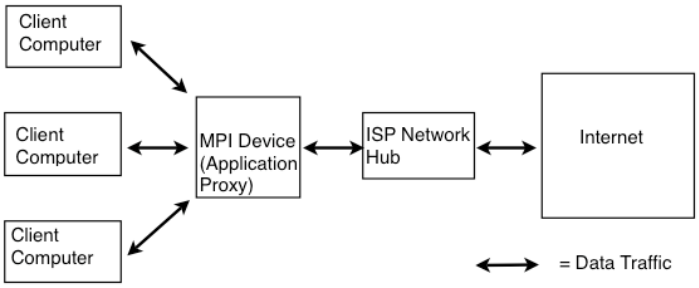


Figure 3: MPI Device Inline with Network Routing Equipment

Using MPI devices, network administrators could prevent client computers from receiving flash files or image files from unencrypted websites. MPI technologies can prioritize some packets over others by examining the application commands that are located within the application layer[35] and the file formats in the presentation layer.[36] Given their (limited) insight into the application layer of the packet, these devices can also be configured to distinguish between normal representations of a data protocol such as HTTP and abnormal representations, and they can filter or screen abnormal representations from being passed to a client within the network. They can also dig into the packet and identify the commands that are being associated with an application protocol and permit or deny the data connection based on whether the command/application combination is on the parse-list. Thus, an FTP data request that included the 'mget' command, which copies multiple files from a remote machine to a local machine might be prevented, whereas FTP connections including the 'cd', or change directory command, might be permitted. Given the status of MPI devices as

[35] Application commands are typically limited to Telnet, FTP, and HTTP.
[36] Thomas Porter, Jan Kanclirz and Brian Baskin, *Practical VoIP Security: your hands-on guide to Voice over IP (VoIP) security,* (Rockland, Mass.: Syngress Publishing, Inc., 2006).

application proxies, they also assume characteristics of offering full logging information about packets as opposed to just header information, and when integrated into a trust-chain can decrypt data traffic, examine it, re-encrypt the traffic, and forward it to the traffic's destination.

MPI devices suffer from poor scalability; 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.[37] Given these weaknesses, MPI devices are challenging to deploy in large networking operations where a large variety of applications must be monitored. This challenge limits their usefulness for Internet Service Providers, where tens of thousands of applications can be transmitting packets at any given moment.

While MPI devices suffer from limitations, they act as a key facet in technological developments towards deep packet inspection. Specifically, their capability to read the presentation layer of the packet's application layer acts as a transition point for reading the entire payload. As a result, this inspection technology constitutes a stepping-stone in the path towards contemporary deep packet inspection technologies.

Deep Packet Inspection

Deep Packet Inspection (DPI) equipment is typically found in expensive routing devices that are installed in major networking hubs. The equipment lets network operators precisely identify the origin and content of each packet of data that passes through these hubs. Arbor/Ellacoya, a vendor of DPI equipment, notes that their e100 devices use DPI "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."[38] Whereas MPI devices have very limited application awareness, DPI devices can potentially "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

---

[37] Chris Tobkin and Daniel Kligerman, *Check Point Next Generation with Application Intelligence Security Administration,* (Rockland, Mass.: Syngress Publishing, Inc., 2004).
[38] Arbor Ellacoya, "Arbor Ellacoya e100: Unmatched Scale and Intelligence in a Broadband Optimization Platform (Datasheet)," Arbor Networks 2009, accessed March 14, 2011, http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=355.

they are typed out by the user."[39] While MPI devices have scaling issues, 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 and behave reactively, insofar as actions against certain data packets can be taken when particular pre-set conditions are met.

At its most basic level, DPI equipment examines a particular packet in its totality and examines the packet's characteristics against a predefined rule set. Such examinations entail looking at layers 2-7 to examine packet headers and payloads to search for indications of protocol non-compliance, malicious code, spam, and any predefined data types that the network owner wants to monitor or take action toward. The equipment identifies and classifies packets based on a signature database. Signatures are developed by extracting characteristic elements from packets that are associated with applications of interest. These characteristics are used to develop signatures in port addresses, string matches, and the packets' numerical properties. Port address analysis behaves similarly to SPI and MPI techniques: the equipment examines which data port is in use and, where that port is uniquely assigned to a single application or protocol (e.g. port 25 is assigned to SMTP email traffic), then packets that are being transmitted to or from the port may have an action taken against them. String analysis entails examining the packet for unique numeric and alphabetic characteristics, such as the name of the application responsible for transmitting the packet. String analysis enables the operator to 'catch' packets that use a common port, such as port 80, to either avoid detection or take advantage of more relaxed rules. Thus, a peer-to-peer application might transmit data using port 80 but, if it declares its name, a string analysis may identify the application's traffic. When examining numerical properties, the DPI device will examine the specific size of the data packet—where very specific sizes are identified and the packet accords with other characters (e.g. port or string) then action may be taken.[40] No specific analytic technique needs to be used in isolation; taken together these variables constitute signatures.

---

[39] Nate Anderson, "Deep Packet Inspection meets 'Net neutrality, CALEA," *Ars Technica*, July 25, 2007, accessed March 20, 2011, http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars.

[40] Allot Communications, "Digging Deeper Into Deep Packet Inspection (DPI)," Allot, 2007, accessed July 28, 2011, https://www.dpacket.org/articles/digging-deeper-deep-packet-inspection-dpi.

Upon identifying a packet-of-interest, DPI equipment can redirect, mark or tag, block or drop, rate limit, or report to the network administrator. A redirection could see particular packet signatures forwarded to a specific location within the network; perhaps all SMTP (email) traffic is forwarded to a specialized piece of equipment that evaluates whether the traffic is spam or not, and then subsequently sends the email to its destination. Packets can also be marked to assign them a quality of service level; packets that are sensitive to high levels of latency, which is the measure of delay experienced in the packet exchange system, might be given a higher priority to be routed to their destination than packets that are less affected by latency. Packet tagging, in contrast, is predominantly used to assign internal identifiers to packets than can then be acted upon. Tagging can often be performed by one device, such as DPI, that can modify packets, and a subsequent element of the network can read the tag and take action based on the tag. This action might include routing the packet through a particular network gateway or only moving it along a particular set of friendly/secure routers. When either blocking or dropping packets, the equipment will refuse to forward the packet to the next hop towards its destination, often without notifying the source of the packet that it is being blocked. Rate limitations establish particular levels of data transmission capacity depending on the application responsible for generating the data traffic. Such limitations are particularly common where certain applications, such as FTP and peer-to-peer, are well known to use large amounts of data capacity (measured in data transferred per second) and data volume (measured in the total amount of data that is being transferred over time).

In some cases, DPI equipment cannot immediately identify the application that has produced a packet. When identification failure occurs, network operators can use 'Deep Flow Inspection' (DFI) technologies to collect packets in the device's short or long memory. DFI lets network administrators perform forensic analysis of packets to determine "the real causes of network problems, identify security threats, and ensure that data communications and network usage complies with outlined policies."[41] Packets can be either fully captured, or have only particular characteristics such as IP destination, the port the packet used or application-type captured. After a DFI process, packet streams

[41] Bivio Networks and Solera Networks, "White Paper: Complete Network Visibility through Deep Packet Inspection and Deep Packet Capture. Lindon, Utah: Solera Networks, 2008, accessed March 21, 2011, www.soleranetworks.com/products/documents/dpi_dpc_bivio_solera.pdf.

can be evaluated against sets of known applications and their corresponding data stream patterns, which lets ISPs evaluate whether their customers are conforming to security or data usage policies. To elucidate, 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 rule sets 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 the memory of the inspection device until it has enough information to appropriately match the packets against the devices' list of known packet-types.[42] 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 DFI technologies and subsequently analyzed using DPI functionality, this activity would substantially slow the transmission of packets and degrade user experiences when they were streaming content. Further, if the network environment has a large number of client devices or users, such as in mid-to-large sized businesses and ISPs generally, the storage requirements would likely prohibit even short-term full data retention. As a result, DFI is not marketed as a means to persistently capture all of the data that ISPs' customers send and receive, but to enable targeted capturing of packets. Such data captures can be used to improve subsequent network performance and to comply with regulatory demands, such as government wiretap or data retention and preservation requests.

DFI capabilities can also be used to compose the unique hash of files that a user is receiving from or transmitting to the Internet. After computing the hash, the device can examine it against a hash database and take action against the file. Hash-based approaches fail, however, when the file itself has been modified in any manner, such as

---

[42] Allot Communications Ltd., "Digging Deeper into Deep Packet Inspection," Allot Communications, Ltd., 2007, accessed March 21, 2011, http://www.cxo.eu.com/article/Digging-Deeper-Into-Deep-Packet-Inspection-DPI/.

when a word processing file has text added or subtracted. Fingerprinting is a more computationally intensive process, which entails generating a unique representation of the file that is being monitored for and examining the file that passes through the DPI appliance – not the file's hash – to see if the representation is present. As a result, in the case of a word processing document, the DPI device would identify a modified file by reference to the common fingerprinted data that was shared between the original (unmodified) document and the modified one. Such processing is extremely expensive, however, and is presently ill suited for large-scale fast network conditions.[43]

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 the device 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.

To make this latter process a bit clearer, let us turn to an example. Skype, a proprietary voice over IP service and software application, hinders packet inspection devices from identifying its packets by masking its legitimate packet header information and encrypting payload data. Given that the packets themselves are encrypted and the information contained in the headers is bogus, ISPs must adopt a different method for detecting Skype traffic. As a 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 follows a common pattern that can be heuristically identified and correlated with the Skype

---

[43] Klaus Mochalski, Hendrik Schulze, and Frank Stummer, "Copyright Protection in the Internet (Whitepaper)," *ipoque*. 2009, accessed March 22, 2013, http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-copyright-protection-internet.pdf.

application.[44] After the application is identified, DPI devices can impede or prioritize the packets that the Skype application generates.

Effectively, DPI lets network owners inspect, stop, or manipulate unencrypted data exchanges flowing across their network in real time. Where encrypted data is transferred using a known pattern, administrators can intuit what is likely transmitting the data and similarly take action. This level of awareness concerning packet contents lets administrators interact with packets at a granular level, and in an automated fashion, before the packets leave the originating network or arrive at a recipient within that network. This interrogation capacity has implications for how large network providers, such as Internet Service Providers (ISPs), develop their network and also establishes an appealing technical infrastructure that non-ISPs may be interested in influencing. Having discussed the capabilities of deep packet inspection, let us turn to how they might be utilized to fulfill various technical, economic, and political goals.

Technical Capabilities and Their Potentials

Deep packet inspection devices are designed to accomplish a range of goals; they are deployed for security, network management, content identification, and data modification purposes. A range of socio-political potentialities is integrated into the design of the technology and is responsible for driving its characteristics and technical capacities. While more detailed investigations into the theory of social-technical relationships, and empirical data on actual uses of deep packet inspection will follow in later chapters, I first discuss the potentialities linked with the technology. To this end, I suggest that there are technical, economic, and political uses to which the technology may be put.

The Technical Possibilities of DPI

Network administrators are concerned with the functioning of the network itself: are security incidents logged and kept to a minimum? Do network policies simultaneously ensure the functioning of the network and meet users' expectations and needs? Are the

---

[44] Dario Bonfiglio et al, "Revealing Skype Traffic: When Randomness Plays With You," *Computer Communications Review* 37(4) (2007): 37-48. Peter Renals and Grant A. Jacoby, "Blocking Skype through Deep Packet Inspection," *42nd Hawaii International Conference on System Sciences* (2009). See also: Allot Communications Ltd., "Digging Deeper into Deep Packet Inspection," Allot Communications, Ltd., 2007, accessed March 21, 2011, http://www.cxo.eu.com/article/Digging-Deeper-Into-Deep-Packet-Inspection-DPI/.

network's nodes appropriately configured to address congestion? Deep packet inspection helps administrators improve network security, implement access requirements, guarantee quality of service, and tailor service for particular applications. Each of these functions is dynamic, insofar as the technology can utilize layered rule sets and is incorporated within a broader networking assemblage to dynamically react to changes in the network. As a result of DPI's penetration into packet transfers, combined with its potentialities, the technology can be helpful in daily and long-term network operations.

DPI was initially meant to offer network providers improved intrusion detection and prevention mechanisms that could recognize and respond to contemporary threats.[45] To respond to emerging threats, DPI appliances are reconfigurable and can scale to monitor high volumes of traffic and to provide logging and anomaly detection. Logging establishes a pattern of known behavior and lets the system (and system administrator, if they examine the logs) examine traffic 'offline'. Offline analysis facilitates a granular analysis of the traffic because it needn't occur in real time, thus mitigating some of the technical challenges associated with in-depth analysis of data packets while maintaining high data-transit speeds. As a result of logging traffic, systems and administrators can 'learn' how to sub-classify network traffic within applications. To make analysis process a bit clearer, consider a process of logging unencrypted HTTP, or web browser, traffic. The system could identify HTTP traffic, and then sub-classify traffic associated with social media websites, further classify traffic to differentiate between downloading and uploading traffic, and go one step further by identifying whether a user is involved in transmitting or receiving images, movies, or other types of content within a social media website.[46]

It is also possible to use logging-based learning to develop expected use-patterns for individual users and applications and to send notifications to administrators if deviations from the norms are detected. Such deviations may indicate that a known client's credentials are being used by a third-party to access the network, based on suspicious or deviant data transmissions and receptions, or that an application has been infected with malware. Because DPI systems afford high levels of control, if a particular

---

[45] Ioannis Sourdis, *Designs & Algorithms for Packet and Content Inspection* (Delft: TU. Delft, 2007).
[46] This level of functionality is provided by Q1 Labs' 'QRadar 7.0' product.

detection signature is too 'chatty' – if a signature is being identified regularly but is uninteresting to the network administrator – the DPI system can be set to either ignore or more carefully monitor the signature in question. A more careful monitoring schema might narrow down the parameters of the inspection, such as shifting from monitoring for all encrypted communications across a corporation to monitoring for encrypted communication in specific business units that are not expected to engage in secure communications.[47] Alternatively, the system might be set to avoid establishing a 'normal' activity pattern for authenticated 'guest' accounts because the logged in user(s) regularly changes, though the equipment could still watch for anomalous application behavior.

More generally, as a component of an integrated security processes, DPI can examine inbound and outbound data traffic and flag packets that warrant a more sustained analysis of their contents. This flagging might happen when the device cannot positively identify the application responsible for the packet or when the device is configured to forward some packets to a proxy server prior to delivery. At the intermediary between the DPI appliance and destination, an algorithmic analysis may be performed. Such an analysis might examine whether an email attachment contains material that cannot enter or exit the network or might generate an alert requiring a human to evaluate the information, such as when abnormal packets are being received or transmitted,[48] or to vet the appropriateness of email attachments.[49] When directing data traffic beyond the network that the DPI is integrated into, the DPI device might add a prefix to a packet's header to indicate the quality of service it should receive, whether the packet is the bottom of a 'stack' or series of related packets, or the device might impose a

---

[47] This specific attention to encryption from systems and business units that have not been configured to use encryption by IT staff is a reasonably common practice in some businesses in Canada. This kind of activity is monitored because abnormal instances of encrypted data traffic may indicate that either an employee is engaged in espionage or (more commonly) has established an encrypted proxy connection to evade business policies and watch online television or download movies.

[48] A properly configured DPI device may have been helpful in diagnosing a problem with network equipment run by Telekomunikacja Polska, Poland's national telco. They had network equipment that was mangling traffic by stripping TCP headers from the packet payload, which resulted in their network transmitting unusual and suspicious traffic to ports 21536, 18477 and 19535. Had DPI been in place at the outskirts of their network, the telco might have identified the traffic and corrected its implementation of TCP/IP itself, rather than relying on third-party researchers to identify the packets and their source. For more on this, see Michael Zalewski, *Silence on the Wire: a Field Guide to Passive Reconnaissance and Indirect Attacks* (San Francisco: No Starch Press, 2005), 186-187.

[49] Sonicwall, "10 Cool Things Your Firewall Should Do," *Sonicwall*, 2008, 11, accessed February 3, 2013, http://www.sosonicwall.com/lib/deciding-what-solution/10_Things_Your_Firewall_Should_Do.pdf.

time-to-live value[50] that overwrites the value set by the client sending the packet. Stacks of tags might nest a series of attributes, such as Quality of Service or where the packet should be forwarded, and may be coded so that egress or ingress networks can act on the attributes.[51] Such prefixes can also be used in establishing virtual private networks when partnered with perimeter edge routers that can maintain their own routing tables. Perimeter routers will identify what other routers traffic can be forwarded to, and they separate traffic so that users cannot see data outside of their network. Using this approach, encryption is not required because traffic cannot deviate from pre-programmed traffic routes.[52]

Existing policy management tools and servers will often guide the technical management of data traffic. Policy control is "a broad concept" that "is usually based on the use of an automated rules engine to apply simple logical rules which, when concatenated, can enable relatively complex policies to be triggered in response to information received from networks."[53] Network managers can examine which account is authenticated to a particular data stream, call the rules dictating how that user can transmit and receive data, and then examine the entire packet stream and mediate data flows as dictated by the policy governing the user. This management capability may mean that an ISP's entry-level client is prevented from transmitting any packets that are unrelated to HTTP (web-based) or SMTP (email-based) traffic, whereas premium users have all of their data traffic prioritized over that of other users of the network. Policy controls permit a vast range of rules, which may prioritize or deprioritize specific kinds of traffic either in perpetuity, at certain points in the day, or for certain users. Policy

---

[50] Time-to-live (TTL) is a value that identifies the maximum number of 'hops' that a packet can take before the Internet's routing structure will cease to pass it to another router. It is meant to prevent endless loops of packets being sent through the Internet – thus consuming router resources – when something has gone awry with routing tables. Each packet has a number assigned to it by the client application, in tandem with the client computer's implementation of the TCP/IP stack, and that number decreases by one for each 'hop' to a new network component that it travels along.

[51] Yakov Rekhter et al., "Tag Switching Architecture Overview," *Proceedings of the IEEE* 85(12) (1997).

[52] Cisco, "Introduction to Cisco MPLS VPN Technology," in *MPLS Solution User Guide*, accessed June 26, 2011, http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html; Kelly DeGeest, "What is an MPLS VPN Anyway?" *SANS Institute*, 2001, accessed June 25, 2011, http://www.sans.org/reading_room/whitepapers/vpns/mpls-vpn-anyway_718; Eric Rosen and Yakov Rekhter, "RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNS)," *IETF*, 2006, accessed June 25, 2011, http://tools.ietf.org/html/rfc4364.

[53] Graham Finnie, "(Report) ISP Traffic Management Technologies: The State of the Art," *CRTC*, 2009, accessed June 27, 2011, http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm.

controls can block some content if the user's account does not permit its reception or transmission, or they can modify some data traffic in real time. Modifications might include changing HTTP traffic so users see a banner that notes that they are nearing or exceeding the volume of data they are provided within a billing cycle[54] or warning them that they might be infected with a virus, worm, or other piece of malware in their web browser. The policies, and their associated servers, work hand-in-hand with DPI devices, often guiding how the devices themselves take action on packets traversing the network.

Digital networks are involved in transmitting more and more data, and key points in the network require regular upgrades to keep pace with growth patterns. While growth adheres to a well-known rate,[55] the general patterns of aggregate expanded bandwidth requirements do not necessarily identify the expanded bandwidth requirements placed on particular routers. When routers experience high-levels of usage – when so many data packets are sent to a router that it reaches or exceeds the maximum amount of packets it can forward to the next hop per second – they become congested. Congestion simply means that, for a period of time, more data is forwarded to the router than it can pass forward. As a result, some packets are not forwarded to their next hop on the Internet and thus are not delivered to their destination.[56]

Deep packet inspection equipment can be used to mitigate the inconveniences associated with router congestion. By identifying and prioritizing packets in real time, DPI appliances can ensure that time-sensitive packets, such as those associated with voice over Internet protocol (e.g. Skype) communications, are moved up in the 'queue' of packets and those that are less sensitive, such as email, are dropped to be resent. Alternately, if the network operator has identified particular applications or application-types that significantly contribute to router congestion, particular rules can be established to limit the amount of the router's bandwidth they can consume. Thus, 20% of a router's

---

[54] One Internet service provider in Canada, Rogers Communications, currently modifies data traffic to alert customers when they are nearing their permitted monthly data volume allowance.

[55] The Minnesota Internet Traffic Studies research group and Cisco alike publish expected bandwidth growth rates, and both typically project roughly similar rates. For more, see: http://www.dtc.umn.edu/mints/

[56] It is important to note that dropped packets are a common event in digital networks. Each packet has a sequencing number and when a client does not receive a packet it will request that the packet be resent. Resent packets may take an alternate pathway to their destination, thus avoiding the previously congested network link.

aggregate bandwidth might be allocated to the 'problem' application or application-type, and the remaining 80% of aggregate bandwidth might be available to all other data traffic. The administrator could forgo assigning bandwidth to any particular application and instead limit the amount of bandwidth that it could consume. Such limitations would restrict the associated application's potential data rates and, as a result, lessen 'problematic' applications' contributions to router congestion. These techniques have raised concerns: there is a fear that analyzing packets using DPI to assign packet priority levels may actually worsen congestion by ultimately requiring higher levels of packet retransmission than would occur without DPI-enhanced analysis[57] and that such analysis may not identify the real cause of congestion, the expansion of router buffers to hold more and more packets for transmission instead of dropping them more rapidly.[58] Such concerns have not prevented network administrators from installing DPI equipment in their networks or from monitoring and acting on data packets.

In the previously noted approaches, the network operator has made some kind of decision about the appropriateness of the applications that end-users are employing: either some applications are more important than others or are identified as problematic and thus have special rules crafted to mediate their ability to generate congestion. Using DPI, a network operator can also shift focus from the application to the user. In this situation, an administrator might establish conditions concerning how clients can utilize available bandwidth. As an example, when a client has used its maximum allotted bandwidth for a 15-minute interval, it might have *all* of its traffic deprioritized or delayed for a period of time following the interval. This action has the effect of prioritizing 'bursty' traffic, that which transmits data in short intervals rather than over a long period of time. Accessing webpages generates bursty traffic, whereas long file transfers using either peer-to-peer applications or a file transfer client are non-bursty types of traffic. This user-centric approach can be seen as 'application agnostic', insofar as it does not

---

[57] M. Chris Riley and Ben Scott, "Deep Packet Inspection: The end of the Internet as we know it?" *Freepress*, 2009, accessed June 18, 2011, http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf.

[58] The expansion of router buffers to hold more packets is referred to a 'bufferbloat' and causes high levels of latency which may, in turn, worsen Internet connections. Bufferbloat afflicts both client devices, such as home computers, mobile phones, and anything else with a TCP/IP stack, as well as routing devices. For more, see Jim Gettys, "Bufferbloat: Dark Buffers in the Internet," *IEEE Internet Computing* 15(3) (2011). The project investigating bufferbloat is online at http://www.bufferbloat.net/projects/bloat.

target specific applications, though the rule set will disproportionately affect some applications, such as peer-to-peer and FTP clients, over others, such as web browsing. Taken together, it is apparent that DPI equipment provides network administrators with tools to better secure their networks, implement access requirements, and modify quality of service for some applications. Whether this control is a prominent driver for the actual *adoption* of these technologies will be explored in subsequent chapters.

The Economic Potentials of DPI

The ability to examine and act upon data packets in real time affords new revenue opportunities for ISPs and third parties alike, as well as offering ways to curtail threats to revenue maximization. Specifically, Internet service providers may be motivated to offer differentiated service plans that compete based on what applications customers can use to connect to the web, the priority that applications' packets are given at routers, or the speed at which users can access websites. ISPs may also prioritize their own 'value added' services, such as voice over Internet protocol, email, or home security systems, over services offered by their competitors. Parties other than network owners may also be interested in DPI: copyright holders may try to limit the sharing of files that infringe on copyrights, and advertisers may monitor and mine data traffic to identify consumer habits and subsequently modify packets to serve targeted ads.

ISPs have offered differentiated service plans since dial-up modem pools were used to connect to the Internet. Today, broadband connections mean that ISPs compete based on the rate that data is exchanged between the client's location and the Internet, the volume of data they are permitted to transfer each month, value-added services such as email accounts, and cost of service delivery. DPI lets ISPs further distinguish their offerings by selectively letting applications connect to the Internet; a web browser and email client connection might be included in a 'basic' Internet package, whereas video game applications or streaming music applications might be included in a 'premium' package. The fungibility of DPI and deep integration with policy control servers afford advantages over prior networking technologies, such as MPI, insofar as the same device is better able to mediate multiple different data forms and formats. Further, whereas some data types, such as web traffic, or data sources, such as a national online newspaper,

might not be counted towards a monthly data quota, other data types and sources could.[59] Alternatively, an ISP could limit or prevent access to the Internet unless customers pay for each connected device; DPI can be used to examine data traffic and ascertain whether 'registered' or 'unregistered' devices are attempting to access the Internet and, in the case of unregistered devices, limit their access until a fee is paid. Figure four gives a theoretical example of what these kinds of pricing formats might look like.

Figure 4: A Tiered 'App-Based' Pricing Model for the Internet

This limitation by device is part of an 'app-model' for the Internet, where connectivity is bundled with a particular application, such as an online movie watching application, or a particular device, such as a PC or tablet computer. In an app-based model, users may never see how much bandwidth volume or capacity they are afforded and instead enjoy only selective access to the Internet based on the services paid for on a monthly basis.[60] This approach to Internet pricing might be combined with, or supplemented by, a prioritization of an ISP's own services to the detriment of competitors. The ISP's voice over Internet protocol client, or a client belonging to a company that had paid an ISP, might be 'free' with the basic package whereas competitors' VoIP traffic is given a lower priority. This approach could buttress an ISP's complementary products or enhance revenue when competitors pressure those

[59] For a brief report on these kinds of differentiations of service, see Nate Anderson, "Can ISPs charge more to make gaming less laggy? They already do," *Ars Technica*, December 15, 2010, accessed March 22, 2013, http://arstechnica.com/tech-policy/news/2010/12/can-isps-charge-more-to-make-gaming-work-better-they-already-do.ars.

[60] Nate Anderson, "Imagine a world where every app has its own data plan," *Ars Technica*, December 15, 2010, accessed March 22, 2013, http://arstechnica.com/tech-policy/news/2010/12/net-neutrality-nightmare-a-world-where-every-app-has-its-own-data-plan.ars.

complementary product lines.[61] DPI could be used to identify favored applications and give them preferential treatment by guaranteeing higher levels of priority, making larger volumes of bandwidth available to them, or by not counting the data they generate against users' monthly volume limits. An ISP's exclusion of competing services or rent-seeking may be logical from the stance of economics. More specifically, "[a]s long as the exclusion of rivals from its Internet-service customers translates into more sales of its complementary product, and the additional profits are larger than the costs of exclusion, exclusion will be a profitable strategy."[62] Given the relative prevalence of viruses, malware, and spyware the exclusion of competing applications may be couched simultaneously in the languages of service and security, which mask the core economic drivers behind the facade of technical improvements to the network.

DPI also provides copyright holders with a tool to (try to) limit or monitor the traffic of infringing computer files and data streams that course across the Internet. To date, most analyses of infringing data traffic rely on questionable statistics or shoddy methodologies. In the case of the former, the United States' Government Accountability Office (GAO) has publicly rebuffed the monetary losses that American corporations claim to experience from infringement. The GAO notes that for widely cited statistics no studies exist that support estimated losses, and that efforts to evaluate actual losses suffer from methodological limitations.[63] The introduction of detailed packet analysis equipment begins to resolve some of the methodological problems associated with quantifying infringing data traffic; by monitoring packets and cross-referencing them against their point of origin – are they from 'legitimate' digital retailers – and their contents – do the files contain copyrighted material – it is theoretically possible to develop an index of how much unencrypted data traffic is potentially infringing.[64] If the copyright monitoring system isn't intended to prevent the movement of data, but merely

---

[61] Christopher Parsons et al., "The Open Internet: Open for Business and Economic Growth," in *Casting and Open Net: A Leading-Edge Approach to Canada's Digital Future*, ed. Steve Anderson and Reilly Yeo (2011), Pp. 107.
[62] Barbara van Schewick, *Internet Architecture and Innovation* (Cambridge, Mass.: The MIT Press, 2010), 253.
[63] United States Government Accountability Office, "Intellectual Property: Observations on Effects to Quantify the Economic Effects of Counterfeit and Pirated Goods," (United States Government, 2010).
[64] Christopher Parsons, "Aggregating Information About CView," *Technology, Thoughts, and Trinkets,* December 17, 2009, accessed March 22, 2013, http://www.christopher-parsons.com/aggregating-information-about-cview/.

log it, a DPI system could be established to do a quick analysis of packets to identify their likely contents. Where it identifies the packets as potentially holding infringing content, they could be passed to their destination, while copies are made and stored in a short-term offline storage system. Once in that system, a computer program could develop a hash value for the files and compare it against a known list of copyrighted files. Where the file was protected under copyright and the source of the transmission was an illegitimate online content provider, the storage system could call on the subscriber database, correlate the subscriber's personal information with the inappropriate exchange of infringing material, and notify an ISP administrator or member of council, copyright holders, authorities, or some other designated party.

One problem with using a hash-based analytic system is that minor changes in the file can result in different values being generated.[65] These values would not align with the database of known hashes, and thus the DPI or offline analysis system would not identify the files as potentially infringing. To identify files that have had slight modifications or elements of files that have been combined to create a 'mash-up' of multiple content sources, file fingerprinting could be employed. Because fingerprinting is a computationally expensive process it is not tenable to fingerprint files in real time. It is, however, useful for offline search and analysis of files.[66] If DPI was used to 'prescreen' data traffic that might be mobilizing infringing data – perhaps targeting applications and application-types that are believed to be prominently involved in moving infringing material – an offline analysis, tied to a database with content fingerprints and subscriber database associated personal information with instances of infringement, could be used to monitor and react to the transfer of copyrighted content.

---

[65] It should be noted that, while small changes can modify a hash value, for most infringing works there are 'only' 3-6 popular variants on the Internet at any time. While further changes might prevent perfect monitoring and enforcement of copyright-related policies, arguably a significant amount of infringing data transfers could theoretically be identified. For more, see: Klaus Mochalski, Hendrik Schulze, and Frank Stummer, "Copyright Protection in the Internet (Whitepaper)," *ipoque*, 2009, accessed March 22, 2013, http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-copyright-protection-internet.pdf

[66] Klaus Mochalski, Hendrik Schulze, and Frank Stummer, "Copyright Protection in the Internet (Whitepaper)," *ipoque*, 2009, accessed March 22, 2013, http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-copyright-protection-internet.pdf, 4.

Alternatively, if copyright holders have identified a particular application or protocol as principally involved in exchanges of copyrighted material then they might demand that DPI equipment scan packets for that application or protocol. Upon detecting 'suspicious' packets, the equipment might block the packets, degrade their priority levels, delay their transmission speeds, or inject 'reset' packets into the data stream. By injecting reset packets a connection between clients is terminated, thus ending the transfer of potentially infringing data between the clients involved in the transaction.[67] Resetting connections between applications can also be used to disrupt large-scale data transfers that are believed to contribute to congestion at nodes in the network.[68] While copyright holders may be independently motivated to 'encourage' using DPI to address copyright infringement, such motivations may be enhanced where network operators are *also* rights holders. In such a case, limiting copyright infringement might be positioned as ensuring user security – protecting users against malware-ridden files integrated with music files users are interested in – as well as ensuring 'appropriate' and 'fair' uses of the network, all while protecting content-based revenue streams that might be reduced by copyright-infringing behaviors.

The injection of foreign code into data transfers can also facilitate enhanced behavioral advertising systems. Behavioral advertising is the "practice of tracking consumers' online activities to target advertising to individual consumers based on their online history, preferences and attributes."[69] When DPI is used to facilitate advertising, it can modify data packets that customers request from the Internet and add a tracking code to otherwise legitimate data traffic. In the case of such practices, monitoring users' online transactions demands tracking online behaviors ways that users cannot prevent. The process of modifying data streams and packet contents to inject tracking code is only

---

[67] RadiSys, "DPI: Deep packet inspection motivations, technology, and approached for improving broadband service provider ROI," *RadiSys* (2010), http://www.radisys.com/Documents/papers/DPI_WP_Final.pdf, 3. For a discussion on detecting packet injections, see Seth Schoen, "Detecting Packet Injection: A guide to observing packet spoofing by ISPs," *Electronic Frontier Foundation*, November 28, 2007, accessed March 22, 2013, https://www.eff.org/files/packet_injection.pdf.

[68] M. Chris Riley and Ben Scott, "Deep Packet Inspection: The end of the Internet as we know it?" *Freepress*, 2009, accessed: June 18, 2011, http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf. 4-5.

[69] Janet Lo, "A "Do Not Track List" for Canada?" *Public Interest Advocacy Clinic*, October 2009, accessed March 22, 2013, http://www.piac.ca/files/dntl_final_website.pdf, 4.

possible using technologies that penetrate the payload of a packet, and this is only possible using DPI-based technologies.

The Political Potentials of DPI

States have been monitoring and analyzing citizens' telecommunications since the telegraph, to the point of retaining encrypted text and banning certain modes of communications for fear that they would undermine state surveillance. DPI lets network operators monitor communications remotely and in real time for content of interest. Given its capacity to monitor the content of communications, DPI can be helpful in supporting 'lawful access' legislation and limiting the transmission of content the state has outlawed.

Lawful access legislation enhances policing and intelligence powers. There are typically three types of access powers associated with such legislation: search and seizure provisions, interception of private communications powers, and production of subscriber data.[70] Deep packet inspection equipment is most useful in intercepting communications, and can be thought analogously as installing wiretap capabilities into digital networks.[71] By installing DPI routers at key points in ISPs' networks, it is theoretically possible to remotely monitor communications of those suspected of engaging in illegal acts by making copies of all data traffic or specifically targeting one type of traffic (e.g. VoIP, web browsing, or peer-to-peer) and not logging or monitoring traffic that falls outside of the specified rule set. It is important to recognize that, while using DPI might be seen as the logical technology to facilitate state-based surveillance, this mode of monitoring differs from traditional wiretapping capabilities because of the breadth of communications that occur online. Whereas a traditional wiretap would capture voice communications, DPI-facilitated surveillance can capture and perform front-line analysis on *any* type of digital transaction, be it a voice communication, text-based chat, web-browsing session, or any other kind of non-encrypted transmission. As such, DPI-based 'wiretapping' arguably stretches what it meant by wiretapping to a considerable degree,

---

[70] CIPPIC, "What is "lawful access?" *CIPPIC*, last updated June 2, 2007, accessed March 22, 2013, http://www.cippic.ca/en/lawful-access-faq.

[71] S. Lerman Langlois, "Net Neutrality and Deep Packet Inspection: Discourse and Practice," in *Deep Packet Inspection: A Collection of Essays from Industry Experts* (Ottawa: Office of the Privacy Commissioner of Canada, 2009), 25-26.

and it may not constitute 'maintenance' of state surveillance powers but an expansion of these powers.[72]

As private copyright holders may be motivated to monitor for infringing files coursing across digital networks for civil reasons, the government may be concerned with monitoring and preventing content transmission it has deemed illegal. Using techniques similar to those exercised to monitor for copyright infringement, but with policies designed to take action on data traffic rather than just watching the wire for it, government could try to blacklist files known to contain child pornography, viruses, malware, disapproved encryption protocols, confidential or secret government documents, and so forth. Blocking or monitoring content could take the form of a government requiring certain routing equipment be installed in network providers' infrastructure or demanding that those same providers install and operate the equipment on the government's behalf. Moreover, such analysis and identification requires massively monitoring communications streams. Such actions do not focus on specific individuals, as with a wiretap.

The political capacity to monitor, mine, and censor for certain data traffic will almost certainly depend on framing. Governments have historically used the language of safety, security, and order to justify blocking communications content. This language of "securitization," a process whereby issues, problems, and phenomena are defined in "security" terms and associated with a "protectionist reflex" can be used to legitimize extraordinary means to solve a perceived problem.[73] While state agents could be responsible for ensuring that content is appropriately mediated, it is possible that the same end – blocking content – could be achieved by a shift towards intermediary liability.

Under such a liability approach "the *intermediaries*, or companies transmitting or hosting users' communications or other content, are held *liable* for their users' and customers' behavior."[74] As noted by Morozov, intermediary liability is attractive to

---

[72] Policy Engagement Network, "Briefing on the Interception Modernisation Programme," *London School of Economics and Political Science,* 2009, http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf.
[73] Ulrich Beck, *World Risk Society* (Cambridge, UK: Polity, 1998).
[74] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012), 93.

government because "[i]t's the companies who incur all the costs, it's the companies who do the dirty work, and it's the companies who eventually get blamed by the users."[75] Companies' awareness of their technical capabilities, combined with their (perceived) protection from individual complaints about violations of freedoms of speech and association, can make them the ideal party to which to outsource Internet censorship. Of course, a widespread shift to this liability structure – where ISPs are held accountable for what their subscribers transmit and receive – would constitute a significant transition away from common carrier protections.

Such protections, in theory, immunize ISPs from legal liabilities for what their subscribers transmit so long as the ISPs themselves are not aware of what their networks are carrying. A shift towards ISP liability, however, would effectively mandate awareness of what traffic is being carried. Such a shift might serve to largely formalize already existing practices: today social networking companies, ISPs, journalism sites, and other interactive content communities often censor or block the sharing and posting of content deemed offensive or problematic by the organization in question. Scaling the magnitude of what is blocked or reported to authorities and formalizing the existence of such policies may constitute a quantitative shift but not necessarily a qualitative one in terms of the kinds of actions undertaken.

When simultaneously considering the technical, economic, and political potentialities of deep packet inspection technologies it's helpful to keep in mind that the potential uses of the technology may not necessarily be practically *instantiated* in real-world networking situations. Further, some of the "pure" technical capabilities are infused with the values of control and awareness of the network, and those advocating that the technology be used to meet technical, economic, or political goals may differentially express such values. It is only as I move into the case studies, however, that I will ascertain both the specific drivers and configurations of technologies *as well as* whether the potentialities of the technology can be, or are being, practically instantiated in the real world.

---

[75] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011), 101.

Conclusion

While packet inspection technologies are not new in and of themselves, their newest iteration carries with it advances that may broadly affect digital communications networks. Whereas SPI and MPI let network administrators stop content from reaching clients and provide varying levels of packet awareness, DPI restructures the possible range of surveillance that Internet subscribers may be subject to by extending how, why, and to what extend data communications can be monitored and acted upon. As we will see, DPI has (re)invigorated economic, cultural, and political discussions surrounding the monitoring, censoring, and modifying of the content of communications in real time. DPI's technical potentials have excited a series of prospective policy actors, which operate with different aims and objectives but are mutually interested in framing DPI's usage so that long-term policy decisions reflect each actor's particular interests and goals.

Depending on how it is actualized, DPI may function as a beneficial technology that assuages security worries and permits limited mediation of bandwidth usage until infrastructure is provisioned to relieve congestion. Alternatively, it could be used to radically undermine the neutrality of networks, where ends have more power over the communications flow than the 'core' that routes data between the networks' ends. There are concerns that DPI could be used to hold ISP subscribers hostage, using the technology to extract higher rents than otherwise possible from content providers[76] or undermine competition between businesses and stymie innovation.[77] The technology could be used to regulate content dissemination, sidestepping legal judgments born of slow court decisions and instead automatically limiting expression.[78] Law enforcement and intelligence services might also abuse the technology, and DPI infrastructures they establish could ultimately create gaping communications security vulnerabilities.[79] The range of potentials accompanying DPI indicate the interests that might drive its practical instantiations and remind us that technical artefacts "affect us not merely by dint of

---

[76] Barbara van Schewick, *Internet Architecture and Innovation* (Cambridge, Mass.: The MIT Press, 2010).
[77] Christopher Parsons et al., "The Open Internet: Open for Business and Economic Growth," in *Casting and Open Net: A Leading-Edge Approach to Canada's Digital Future*, edited by Steve Anderson and Reilly Yeo, 2011, http://openmedia.ca/files/OpenNetReport_ENG_Web.pdf.
[78] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, Mass.: The MIT Press, 2010), 188.
[79] Susan Landau, *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (Cambridge, Mass.: The MIT Press, 2011).

physical or material properties but by properties they acquire as systems and devices embedded in larger material and social networks and webs of meaning."[80] Within such larger networks and webs, DPI could even have an effect on the quality of the deliberations between citizens in democratic states: if certain kinds of communications were blocked or delayed, or others accelerated or otherwise privileged, the appliances and their associated policies could 'nudge' democratic discourse in certain discussions.

In light of the *potential* implications associated with this technology, it is important to evaluate the *actual* uses and anticipated potentials of the technology. Moreover, it is important to ask whether implementations of the technology are uniform and, if they are not, what particular social, economic, and political conditions have mediated the application of the technology. To ascertain how and why DPI is deployed and governed, I will, in the next chapter, consider how path dependency, international governance, and domestic policy activities may or may not advance Internet-related policies and practices, and where DPI may figure into each framework. I follow these frameworks with case studies of Canadian, American, and United Kingdom (UK) agendas associated with DPI, studies that will identify which potential uses of the technology have been, or are planned to be, instantiated. It is only after unpacking the reality of DPI deployments that it will be possible to understand the actual, rather than sensationalized or theoretical, politics that are actually driving the adoption of DPI technologies.

[80] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010), 6.

Chapter 3: Who and What Drives Deep Packet Inspection

Technologies are inseparable from and have implications within and upon the social environments surrounding them. At the same time, sunk costs and network effects can 'lock in' particular social principles and values while excluding competing values. Technology does not operate or unfold in a vacuum, however, and large institutions exist – with specific power structures, principles, and actors – to guide the development of key technology systems. In the context of the Internet, the international bodies associated with its growth – the International Telecommunications Union (ITU), Internet Engineering Task Force (IETF), and Word Wide Web Consortium (W3C) – have often had significant effects on the development of Internet technologies and standards. However, whether early decisions still determine how Internet standards develop, or whether Internet governance bodies can still significantly influence or disrupt how data is encapsulated and transmitted across the Internet remains uncertain, at least with regard to applications of deep packet inspection technologies. Indeed, it could be domestic policy or political efforts that primarily influence how and why DPI is deployed.

This chapter considers how a series of frameworks, which focus on technological paths, international Internet governance, and domestic policy processes, could explain the development of Internet-related practices that have been made possible by novel networking technologies such as DPI. Each of these frameworks draws attention to different actors who themselves may be regarded as driving policies. I first consider relationships between social values and technology, with specific attention to historical versus contemporary contestations of control over the management of data packet transmissions. With this analysis completed it is possible to appreciate how certain paths were established in the early moments of the Internet. I then turn to how the framework of international governance could explain the shaping of key Internet systems and whether Internet governance bodies can influence the deployment of DPI. I conclude the chapter by theorizing how national issues are framed, and how social actors may attempt to frame issues to shape technological developments. Collectively, these frameworks will be used to explain whether early actors and actions taken at the inception of the Internet limited or enabled the developments of DPI in the case studies, whether actors from

international Internet governance bodies have significantly influenced the development or deployment of DPI, or whether domestic agents principally have driven DPI's uptake. From this discussion, three frameworks to investigate deployments of deep packet inspection emerge, frameworks that will be used to explain how and what is driving deep packet inspection technologies in Canada, the United States, and the United Kingdom.

Fixed Paths for the Internet?

Technologies underlying the printing press, radio, and television were and continue to be influenced by normative logics governing their inception, deployment, and adoption. The Internet is no exception. What is less clear, however, is how the values embedded in ARPANET – the early, research-based pre-Internet – by its earliest engineers and developers may still be orienting the development of contemporary network technologies.

This section explores the networking logics and structures that emerged from ARPANET, so we can understand how some technological developments and potentialities of digitally networked systems are better enabled than others. This section focuses on the decisions made by the ARPANET core engineers to identify how their decisions established power relations between users of the Internet and those who maintain the core Internet infrastructure. Subsequently, I outline a framework that is based on path dependency. The framework will be used in later chapters to evaluate whether DPI could have, or is already having, a significant effect on the normative principles – and their associated ideology – that were set in motion with the initial development of the Internet.

Inventing the Internet's Potentials

In the 1950s and 60s, the Pentagon's Advanced Research Projects Agency (ARPA) sought to encourage and support advanced "far out" research.[81] This mandate, combined with a director who was an "evangelist" for time-sharing and remote access to databases, established a well-resourced government body that invested in risky research projects. Many of ARPA's earliest funded projects saw researchers receive expensive computers to conduct local research, but, without methods for easily transmitting information, there

[81] Katie Hafner and Mathew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (Toronto: Simon & Schuster Paperbacks, 1996), 22.

were significant duplications of labor. To better manage research investment, Bob Taylor, the director of ARPA's Information Processing Techniques Office, suggested linking computers together across large distances. To test the feasibility of this project, four nodes would be connected in a test network; success would reduce research investment cost and also improve communications reliability.[82]

While Taylor was appropriating funds for the network, researchers outlined a series of communications systems to meet ARPA's requirements that were undergirded by disparate philosophies of network design. An AT&T research proposal sought to 'harden' its telecommunications network by establishing a polygrid-based network. This network had one node for every few hundred telephone lines, as opposed to the traditional phone network where one node serviced thousands of lines. If a node went offline, an operator at AT&T's single operations center could manually reroute communications traffic.[83] This approach was contrasted with Paul Baran's and Donald Davis' distributed packet-based approaches to communications. With Baran's approach, packets could be routed to their destination independent of one another and of an operator, and they would be automatically rerouted if network nodes were taken offline. Baran's system "had many elements that were specifically adapted to the Cold War threat, including high levels of redundancy, location of nodes away from population centers, and integration of cryptographic capabilities and priority/precedence features."[84] Davies, in contrast, was primarily interested in developing a packet-based system to enable interactive computing and ensure fair distribution of computing resources while simultaneously helping to revitalize a lagging British economy. However, Davis could not convince British governments of the day to fund British packet research; as a result, American research efforts and interests dominated the early development of the next-generation, efficient and redundant, digital networks.

Lawrence Roberts oversaw the ARPANET project and recognized the complexity of implementing a packet-switching network. To simplify the process, developers established 'layers' between technical interfaces that would facilitate better testing and

---

[82] Katie Hafner and Mathew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (Toronto: Simon & Schuster Paperbacks, 1996), 40-42.
[83] Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: The MIT Press, 2000), 15.
[84] Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: The MIT Press, 2000), 39.

debugging practices, as well as ensuring that developments at different levels of the network stack minimally interfered with one another. The packet-based network adopted conceptual elements from both Davies and Baran; it emphasized the division of messages into discrete units of data that were autonomously transmitted to their destination. As implemented by ARPANET's designers, however, packets lacked Baran's emphasis on security: nodes were not placed away from population centers nor was cryptography designed into the network itself. As a result, packets were, and remain, typically unencrypted by default as they cross networks.

As packet-switching networks grew more common, an interlinking protocol that let data cross networks that rely on differing local standards was needed. Cerf and Kahn tackled this problem in their 1974 paper, "A Protocol for Packet Network Intercommunication."[85] Their paper outlined the TCP protocol, which would subsequently be divided into the TCP/IP protocol suite; TCP was responsible for "breaking up messages into datagrams, reassembling them at the other end, detecting errors, resending anything that got lost, and putting packets back in the right order." Internet Protocol, or IP, was responsible for the actual routing of datagrams, the term given to packets sent across unreliable services.[86] Critically, it was the 'ends' of the network and not core networking routers that were responsible for establishing and maintaining TCP/IP connections. This arrangement stood in contrast to circuit-based communications, where telecommunications companies established and maintained the communications channels between parties. The result was that the power to control or manage communications was significantly shifted to end-users.

TCP/IP significantly modified the relationship between telecommunications companies and what flowed across their networks because these companies were no longer responsible for establishing and tearing down dedicated communications lines between the ends of a network. In response to the modified relationship, telecommunications firms developed and proposed their own X.25 standard, which established virtual networks between network routers and guaranteed data transmission

---

[85] Vinton Cerf and Bob Kahan, "A Protocol for Packet Intercommunication," *IEEE Transactions on Communications* 22(5) (1974): 637-648.
[86] Katie Hafner and Mathew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (Toronto: Simon & Schuster Paperbacks, 1996), 236.

quality. Using this standard, telecommunications companies could control packet flows, and, consequently, remove that power from the 'ends', or destinations and origins, of the network.[87]

This early conflict over standards saw TCP/IP win out as a dominant standard because it was more widely deployed than competing standards. This dominance meant that, on the whole, the end-user's computers instead of network routers established and maintained communications networks because trust and control rested with the end user. Significantly, the ends have retained power over managing communications flows, at the expense of telecommunication companies' long-held service models that were based on central control of communications to ensure the quality of communications.

ARPANET's Values and the Contemporary Internet

ARPANET served as a space in which to design, test, and deploy novel approaches to communications principles. Two key assumptions ultimately emerged to underwrite ARPANET and the subsequent Internet: trust-your-neighbor and procrastination is acceptable. The former assumed that those configuring endpoints were competent and trustworthy enough that "they would not intentionally or negligently disrupt the network."[88] The latter assumption rests on "the assumption that most problems confronting a network can be solved later or by others."[89] Saltzer, Reed, and Clark first outlined the latter assumption as such:

> The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)[90]

---

[87] Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: The MIT Press, 2000), 156-161.
[88] Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven: Yale University Press, 2008), 31.
[89] Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven: Yale University Press, 2008), 31.
[90] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-to-End Arguments in System Design," *ACM Transactions on Computer Systems* 2(4) (1984): 277.

Their early formulation, which was somewhat permissive towards networks being fine-tuned or fixed for particular protocols, was modified in subsequent work. Reed and his colleagues wrote in 1998 that, "a function or service 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."[91] With this final formulation, each layer of the network was meant to be implemented independently of each other layer; thus, the content layer would not interfere with the logical transmission protocol layer, nor those two with the physical transport layer.[92] This division of operations means that when a protocol is developed, it depends on other layers, and the other layers could be improved to enhance the protocol's effectiveness, but the protocol designers themselves are not expected to improve the entire network stack. They can procrastinate and let someone else fix and innovate on the other layers. This model stands in contrast to the traditional telephony model, wherein the owner of the transmission layer (i.e. the local telephone monopoly) is responsible for maintaining and developing the entire communications stack.

While the research network's developers focused on different layers and openness to different protocols for enclosing and transmitting data, they were also proponents of interoperable standards that facilitated broad-based communications.[93] Common standards make possible today's distributed and omnidirectional network architecture, and they act as structuring agents that govern the architecture of digital objects online. So long as protocols remain open and transparent and are not intermediated or disrupted by other elements of the network stack or intruded upon by non-ends of the network, data objects can be sent and received by the various ends arrayed around the Internet. The transmission and reception of data objects is compromised, however, when other layers of the networking stack, or a third-party that manages core elements of the physical network itself, intentionally disrupt key Internet working protocols. In effect, when your

---

[91] David P. Reed, Jerome H. Saltzer, and David D. Clark, "Active Networking and End-to-End Arguments," *IEEE Network* 12(3) (1998): 69.

[92] This tripartite division is from Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006).

[93] The Internet Engineering Task Force, established with the assistance of many early ARPANET engineers, now functions as an organization that ensures that standards are available online, free of charge, in order to facilitate the adoption of these open and interoperable standards.

neighbors cannot be trusted and network layers are forcibly blurred together, the Internet's capacity to route data between parties is threatened.

As ARPANET transitioned into the public Internet, a series of values such as openness, accessibility, freedom to create, and freedom to experiment were engrained into the most basic standards underwriting the network. The early Internet benefitted from a common presumption whereby everyone equitably and fairly utilized the renewable but temporally limited computational environment. The design of the Internet's core protocols temporarily settled issues concerning the role of network operators versus end-users, and the design emphasized the importance and value of common open standards. At the inception of the Internet, ARPANET decisions meant that economic and creative innovation at each level of the network – hardware, logical transport, and application/content generation – was possible. The modularity reduced costs by providing a platform where development entailed engineering only fragments for the platform, instead of designing entirely new platforms and networking infrastructures. Development could cost millions or billions of dollars (e.g. deploying a new physical-layer system, such as fibre-optic cable or satellite systems) or practically nothing (e.g. a new email client, file transfer protocol).[94] The independence of network layers let entrenched and emerging developers and companies compete in a telecommunications market that had historically been governed by natural monopolies.

However, whereas the early users of computer networks were technically sophisticated and able to come to consensus on how to address interpersonal and technical problems, this is less the case today.[95] Individuals now increasingly look to engage in pre-defined environments, such as social media and privately-provided content management systems, and they disparage instances where their freedoms to engage with content are disrupted by third parties intruding on such engagements.[96] Given the rise of

---

[94] Barbara van Schewick, *Internet Architecture and Innovation* (Cambridge Mass.: The MIT Press, 2010), 206. Christopher Parsons et al., "The Open Internet: Open for Business and Economic Growth," in *Casting and Open Net: A Leading-Edge Approach to Canada's Digital Future*, ed. Steve Anderson and Reilly Yeo (2011).

[95] Marjory S. Blumenthal and David D. Clark, "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World," in *Communications Policy in Transition: The Internet and Beyond*, ed. Benjamin M. Compaine and Shane Greenstein (Cambridge, Mass: The MIT Press, 2001), 95-6.

[96] Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven: Yale University Press, 2008), 54-61.

untrained users and an ever-increasing breadth of Internet-related threats, endpoints of communication are seen as less and less trusted by operators of networking infrastructures. In this networking environment, many would prefer that the network enforce "good" behavior and guarantee the safe delivery and reception of data packets.[97] Moreover, as new Internet-based applications are developed that possess tight operating requirements (e.g. low latencies, low amount of packet loss) or actively bypass Internet protocols meant to alleviate data congestion problems (e.g. some file sharing protocols, such as early versions of BitTorrent), network operators are sometimes called upon to offer differentiated services to ensure that their customers can enjoy favored communications protocols.[98] Mueller recognizes that it isn't just individual customers or citizens who are interested in empowering network hubs at the expense of the ends; economic and security logics encourage corporate and political bodies to advocate for 'safer' and more controllable and surveillance-ready networks.[99]

Whereas the initial principles of ARPANET called for openness and transparency of protocols, network owners are experiencing increased pressure to understand the data that is traversing their networks and guarantee that some data formats flow efficiently and that others do not. Laws requiring access to telecommunications services have been passed that led to networks being made surveillance- and control-ready.[100] Further, demands to quickly access content have spawned server infrastructures in carriers' networks to speed data to end users, with the effect that content can be easily monitored and blocked.[101] These values, which emphasize a network-centric control over the flow of packets, underlie the development of network intelligence appliances such as DPI. The potentialities of the network are now seen less through the lens of non-profit playfulness and more through the lens of for-profit efficiency, security, and control. There is a

---

[97] Marjory S. Blumenthal and David D. Clark, "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World," in *Communications Policy in Transition: The Internet and Beyond*, ed. Benjamin M. Compaine and Shane Greenstein (Cambridge, Mass: The MIT Press, 2001), 93.
[98] Marjory S. Blumenthal and David D. Clark, "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World," in *Communications Policy in Transition: The Internet and Beyond*, ed. Benjamin M. Compaine and Shane Greenstein (Cambridge, Mass: The MIT Press, 2001), 94-5
[99] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, Mass.: The MIT Press, 2010).
[100] Examples include, in the United States the Stored Communications Act, in the UK the Regulation of Investigatory Powers Act 2000, and in Canada the recently proposed 'lawful access' legislation.
[101] Specifically, Content Distribution Networks are used to place content closer to end-users, to increase the rate at which they can get access to data that tends to be highly sensitive to latency and jitter.

remapping of the political and power-based opportunities in the network; in Chapters Four through Six I will explore, specifically, what some of these attempted remappings look like. The (in)effectiveness of modifying the principles and power to manage packets latent to Internet protocols, however, may be significantly disciplined by technological paths that have been established since the Internet's inception.

How a Technological Imperative Could Explain Deep Packet Inspection

Entrenched Internet standards and protocols enable much of how the contemporary Internet functions. In addition to such 'practical affordances', standards and protocols are embedded with particular values and principles. Emergent from these engineering decisions that are laden with ideological orientations, certain technical development paths have been preferred or foregrounded on the basis that they cohere with previous decisions. In effect, systems under a technological imperative will follow paths based on previously established decisions that are challenging to deviate from. The strongest formulation of such an imperative, technological determinism, theoretically identifies power as within the technology itself and, as such, "reduces power to technologically manageable phenomenon." This strong path "sees technology as developing independent from society, but as inducing certain social effects with necessity."[102] This strong conception of the imperative would associate ideological norms within standards and protocols to the standards and protocols themselves. In the process, this approach would elide the political nature of the researchers' funding, social interests that had guided protocol structure choices, and financial capacities that structured what was regarded as (in)feasible. The issue with technological determinism, however, is that it obscures the role of society, politics, and the economy, and, as a result, ignores the social developmental and social context of technological products, processes, and associated actors.

A more modest approach to a technological imperative adheres to path dependency. I adopt this moderate approach to try and understand how technologies can foreground certain options while excluding others. In path-dependent technological

[102] Christian Fuchs, "Working Paper: Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society," EU FP7 – The Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research Into Action, July 2012, 43.

systems, "history is "remembered" … "Small" events early on may have a big impact, while "large" events at later stages may be less consequential. To put this another way, outcomes of early events or processes in the sequence are amplified, while later events or processes are dampened."[103] Per this framework, changes must overcome a lock-in that is associated with systems that involve high levels of interdependence across a spectrum of uses and actors and where changes to systems would necessarily occur over long stretches of time. According to path dependency, processes are not necessarily fixed in a specific direction in perpetuity – which is a position often attributed to technological determinism – but certain processes are challenging to change in any significant manner after the processes have become well established.

Telecommunications systems, by merit of their wide usage, combined with challenges and expense in modifying core infrastructure fit this definition of 'lock-in'.[104] As a result, the technological imperative of such systems can be understood as possessing characteristics of path dependency. These systems are predicated on common interconnection standards. Consequently, they possess "unique features, particularly because of the strength of network effects." Such effects "make these standards most difficult to change" because of their widespread usage and because of their importance for communication in society, in commerce, and by government.[105] More specifically, the following factors contribute to when decisions, practices, and processes are maintained, or locked in, even in the face of more efficient or generally preferable alternatives:

1. Large set-up fixed costs: if an existing system can be used, helpfully or profitably without significant investment of resources, the existing system may be preferentially maintained.
2. Learning effects: if a new alternative would be accompanied by large learning costs, the existing system may be maintained to avoid the expenditure of resources to learn the new system.

---

[103] Paul Pierson, "Not Just What, But *When*, Timing and Sequence in Political Processes," *Studied in American Political Development* 14 (2000), 75.
[104] Paul Pierson, "When Effect Becomes Cause: Policy Feedback and Policy Change," *World Politics* 45(1) (1993), 610.
[105] Charles Vincent and Jean Camp, "Looking to the Internet for models of governance," *Ethics and Information Technology* 6 (2004), 162.

3. Coordination effects: where a series of individuals coordinate their actions to increase their utility in excess of independent action, they may prefer the existing system to ensure that they can continue to enjoy these coordination – and network – effects.
4. Adaptive expectations: on the basis that individuals and groups may want to avoid choosing 'the wrong' new system, they may continue to use the existing system given its current degree of functionality.[106]

Decisions that are made early on, especially with technical and communications systems, may lead to lock-in for any of the aforementioned four reasons. This condition is politically significant on the basis that infrastructure-based systems can conceal the efforts by designers and power monopolies to lock in certain principles or power relationships. Winner, for example, asserts that we should not reduce analysis to either just technology *or* social forces; instead, we must "pay attention to the characteristics of technical objects and the meaning of those characteristics . . . this approach identifies certain technologies as political phenomena in their own right."[107] It is especially important to focus on technologies that are set in place for prolonged periods of time because they can reify particular political values that have long-lasting effects; when building an interstate highway to prevent public buses – dominantly ridden by minorities – from accessing areas of a city, as happened in the 1920s to the 1970s in New York city, it doesn't make sense to just look at the technology (the bridge) or the social forces (politics, individuals involved in decisions).[108] Instead, a hybrid approach that recognizes the interrelationship of technology and social forces is needed.

In a similar vein, Winner argues that certain myths, which obscure market and social structures and seek to reify structures by way of established rules, are linked to the development of communications technologies. For example, there are .com websites, whereas there are not (at time of writing) .union or .ngo websites. The presence and absence of particular identifiers serves to reinforce certain market-based 'realities' of

---

[106] W. Brian Arthur, from Paul Pierson, "When Effect Becomes Cause: Policy Feedback and Policy Change," *World Politics* 45(1) (1993), 607.
[107] Langdon Winner, *The Whale and the Reactor* (Chicago: The University of Chicago Press, 1986), 22.
[108] Langdon Winner, *The Whale and the Reactor* (Chicago: The University of Chicago Press, 1986), 22-23.

contemporary Internet development, while simultaneously, those realities are masked because novel communications come with languages of 'new politics' that declare the new systems will be emancipatory, establish more egalitarian social structures, and defy politics and power as usual.[109] What is most significant about core communications infrastructure is its very longevity: given the sunk costs and network effects of communications systems, social and political relationships that are embedded and facilitated by the infrastructure may be maintained even in the face of reformed social or political principles or models. Thus, modifying existing protocols could threaten the originating actors' ongoing power to manage packets as well as could 'enrol' all existing and future actors into the new regime.

While the invention of TCP/IP established an 'ends-first' prioritization of communications, this needn't have been the case. There were alternate possibilities (e.g. AT&T's polygrid system or the X.25 protocol), but developers focused on end-based power relationships as they developed basic pre- and post-ARPANET protocols. Though developers' decisions were primarily rooted in addressing technical problems – these decisions were not efforts to undermine the telephone companies – the decisions had a significant ideological effect because they redistributed power concerning who predominantly manages communications in communications systems. As such, basic decisions concerning Internet protocols can be understood as "inherently political" insofar as they manifest, through code, a particular social ordering of power. Scholars such as Joel Reidenberg and Lawrence Lessig assert that digital code and technical configurations can operate as an extra-legal regime. For Reidenberg, technology can let *policymakers* establish "impositions on information flows through technological defaults and system configurations" in service of two alternate goals:

1. Immutable policies embedded in technology standards that cannot be altered
2. Flexible policies embedded in technical architecture that allow variations on default settings.[110]

---

[109] Vincent Mosco, *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge, Mass.: The MIT Press, 2004).
[110] Joel R. Reidenberg, "Lex Informatica: The Formation of Information Policy Rules Through Technology," *Texas Law Review* 76(3) (1998), 565.

Lessig sees digital code as an extralegal mechanism that *private actors* can use to create the equivalent of law by enabling or precluding certain actions. He envisions a "West coast code" that involves federal legislatures debating and passing democratically legitimated laws that can, subsequently, affect digital systems and personal behavior versus an "East coast code" that "has become the product of companies."[111] Given that the architecture of digital systems is increasingly developed, controlled, and run by private interests, the regulatory power of that architecture – embedded in digital code – affords power to those private actors. In Lessig's story, the influence of democratic governance is weakened by the very character(s) of who is, and isn't, involved in the basic architecture-driven means of regulating digital communications networks.

From these authors' writings, protocols adopt a kind of quasi-juridical power because they prefigure the possible and potential by way of how data is – and can be – encoded. Writing specifically about Internet protocols, Hochheiser narrows Lessig and Reidenberg's stances:

> Standards act as the laws of the Internet. To communicate on the Internet, users must conform to the rules of SMTP, HTTP, and other standard protocols. Although penalties for non-conformance are limited to the inability to communicate, by defining what can and cannot be done on the Internet these standards act as laws that limit possible behaviours.[112]

Others, such as Denardis, recognize that protocols embed and inculcate certain power relations; the standards that data is forced to correspond with enable or disable personal privacy, autonomy, and dignity.[113] In aggregate, these scholars' writings suggest that the early developers of the Internet encoded a series of 'laws' by establishing the protocols that they did, and, in the processes, they embedded specific values and

---

[111] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books), 72.
[112] Harry Hochheiser, "Indirect Threats to Freedom and Privacy: Governance of the Internet and the WWW," *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*, (2000), 249.
[113] Laura Denardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, Mass.: The MIT Press).

potentialities into the heart of the Internet. These 'laws' were firmly enshrined in Request For Comments standards documents that were promulgated through the Internet Engineering Task Force, though were rarely explicit in their ideological significance. The redistribution of power to manage communications emerged from decisions concerning functional data structuration and data transit problems; engineering decisions concerning what were 'good' solutions may have been established mostly as the most 'practical' solutions, but the decision of what constituted practicality was informed by broader social conditions.

Although certain technological decisions are invested with particular power relations that are path dependent, this situation does not mean that those decisions and relations are permanently settled. Nor does it mean that all parties will docilely accept and abide by a decision after it has been made. Where there are temporarily passive – though permanently agitated – actors, an action undertaken at a critical juncture can unsettle previously settled decisions and prompt shifts in systems' existing trajectories. Such junctions permit "new trajectories" on the basis that "outcomes are often linked to such decision points."[114] For a new trajectory to be realized, whatever the change is, it has to happen at the right time; "Some events or processes occur "too early"; others "too late.""[115] It is at these critical junctions that a small event can threaten the existing system's stability. Alternately, a "big event" that is late in a path and that doesn't fall at the right time might have a minimal effect on the path's trajectory. Even where a trajectory changes, however, the newly oriented path will tend to adopt, accept, or integrate key precepts of the original system: a junction is not the same as a dislocation, and so it does not constitute a total (re)creation of the system at hand.

Though the Internet appears to have a particular path that saw unencrypted packets, ends-based control over packet management, permission for any device to connect, and the non-interference of applications across packet layers, a disruption might significantly alter the path and attendant characteristics of core Internet functions and practices. Some scholars have investigated whether contemporary innovations in packet

---

[114] Joel Rast, "Why History (Still) Matters: Time and Temporality in Urban Political Analysis," *Urban Affairs Review* 48(3) (2012), 9.
[115] Paul Pierson, "Not Just What, But *When*, Timing and Sequence in Political Processes," *Studied in American Political Development* 14 (2000), 84.

inspection may herald "The End of the Net as We Know It" because the basic principles – and associated power relations – linked with the post-ARPANET Internet could be undone.[116] However, while it is possible that at a critical junction the base characteristics of the Internet might change, it is also possible that the capacity to rearrange such power relations is lacking. We may not, in fact, be at a critical juncture, and, even if we are, the path might be sufficiently entrenched that novel trajectories are ultimately unable to break away from the system's present orientation.

Through the framework of path dependency, then, we might be able to explain how a few situations could unfold. First, it is possible that a novel technical change could be proposed but is not adopted in a significant manner because doing so would invite too high a cost or because it is the 'wrong time'. Such a decision could confirm the thesis that in a path-dependent situation, early decisions have significantly more weight than late decisions. Second, it is possible that a novel innovation or systems change could be proposed and partially adopted in a manner that modifies characteristics of the system without undermining the core principles or structures of that system. In such a situation, we could see a later decision affecting the character of the system without significantly affecting its basic terms of functionality. Finally, a novel innovation or systems change could be proposed and adopted, and it could significantly modify the core principles, structures, and associated characteristics of a system. Should this final expectation be realized, either a rupture of a path-dependent system would be realized or we would have to re-evaluate whether Internet-related systems are indeed strongly path dependent.

In the case studies, in Chapters Four, Five, and Six, I will be able to evaluate whether DPI constitutes a critical junction. Should no change in network properties be seen as the technology is introduced, we might theorize that existing systems and principles have established too high a cost to adopt a novel means of interacting with the network. However, should the technology be adopted – a technology that does have the potential to challenge principles and power relations embedded in core Internet-working protocols – then we can explain whether we are witnessing a minor modification or a significant restructuring of the conditions of the 'path' that the Internet systems and

---

[116] Ralf Bendrath and Milton Mueller, "The End of the Net as We Know It," *New Media & Society* 13(7) (2011).

practices follow. Such modifications do not mean that the Internet would be re-structured or –developed whole cloth, but that many of its underlying characteristics might significantly vary from those it had following its emergence from ARPANET. If, however, significant variations in technological reordering are manifest in our case studies, then this finding might suggest that the path dependency associated with the Internet architectures is weaker than expected, and thus indicate that this framework's explanatory capacities are limited at best.

The Role of International Governance

While decisions during the era of ARPANET – and those made since the emergence of the Internet – offer a story of path dependency, international organizations have tried to influence such paths for decades. The designers of the earliest packet-switching networks have worked for, sparred with, and established international Internet governance bodies, such as the International Telecommunications Union, Internet Engineering Task Force, and World Wide Web Consortium. The previous section of this chapter suggested that protocols could be considered law; if that is the case then standards organization can be seen as quasi-legislative bodies.[117] This section focuses on whether these governance bodies have the *capacity* to influence where power rests in the network (ends versus core) and establishes a framework to evaluate and explain, in subsequent chapters, whether these bodies could have, or are having, *substantial* effects on deployments of deep packet inspection in Canada, the US, and the UK.

The Rise and Roles of International Internet Governance Bodies

The earliest international telecommunications body, now named the International Telecommunications Union (ITU), is responsible for "the regulation and planning of telecommunications worldwide, for the establishment of equipment and systems operating standards, for the coordination and dissemination of information required for the planning and operation of telecommunications services, and, within the United Nations system, for promoting and contributing to the development of

[117] Harry Hochheiser, "Indirect Threats to Freedom and Privacy: Governance of the Internet and the WWW," *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions* (2000), 250.

telecommunications and related infrastructures."[118] More specifically, the Consultative Committee on International Telegraphy and Telephony (CCITT) is responsible for generating standards. The CCITT meets every four years to vote on proposed standards. Approved standards are officially non-binding "Recommendations," but CCITT's standards are typically "automatically adopted as national standards by many member countries."[119] Member nations and representatives of national telecommunications carriers have historically dominated the CCITT. The ITU has typically placed emphasis on telephony, rather than computing.

The strong emphasis on cooperation between nation-states combined with the need for government representatives to sponsor non-governmental actors before they can join the ITU have limited the organization's involvement with key Internet standards, standards that were principally developed by engineers associated with ARPANET. While ARPANET engineers were developing Internetworking standards outside of the ITU in informal working groups, conferences, and mailing lists, rival groups associated with the ITU sought to shape Internet-working standards by turning "to their respective preferred standards organizations for the creation of specifications that they hoped would control the future development of networking."[120] This rival development of standards was highlighted when the CCITT proposed protocol, X.25, which concentrated network functionality in parts of the network that were controlled by traditional telecommunications carriers. Such control was at odds with key Internet engineers' situations of power to manage network communications at the end points of the network vis-à-vis their network architectures and designs.

In contrast to the CCITT,[121] the research community that developed the core internetworking techniques, technologies, and standards during ARPANET's operation as a research network gradually coalesced around the Requests for Comment (RFC) document. Germane RFCs were, and still are, used to coordinate and share information amongst some members of the Internet engineering community. Written for, and by, the

---

[118] Susan K. Schmidt and Raymund Werle, *Coordinating Technology: Studies in International Standardization of Telecommunications* (Cambridge, Mass.: The MIT Press, 1998), 48.
[119] Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: The MIT Press, 2000), 150.
[120] Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: The MIT Press, 2000), 151.
[121] The CCITT has since been renamed to the ITU Telecommunications Standardization Sector (ITU-T).

founding engineers and developers of the Internet, RFCs describe merits and flaws of different protocol choices.[122] RFCs are now under the auspices of the Internet Engineering Task Force (IETF), itself associated with the Internet Architecture Board (IAB).

The IETF was created in 1986 and serves "as the primary standards organization developing Internet Protocol drafts." The organization ostensibly functions as an organic community that lets ideas "percolate up from the IETF working groups" to the Internet Engineering Steering Group, which is ultimately "responsible for presenting Internet draft standards to the IAB for ratification as formal Internet standards."[123] Task forces within the IETF have been responsible for essential standards and policy development work, with end-to-end services, privacy, security, network and host interoperability, robustness, user interfaces, and scientific requirement task forces established over its history, amongst others.[124]

A guiding mantra for the IETF is that its members "believe in: rough consensus and working code." This mantra, taken from the experience of developing and running ARPANET, was adopted as the contemporary public Internet built out, and as new protocols and data transmission algorithms were outlined and presented to the Internet community. As a standards body, albeit one without formal rule-making power, the IETF's members investigate, respond to, and develop protocols that are meant to maintain the Internet's ongoing processes and development.

While the IETF can move more rapidly and has a more inclusive membership process than the ITU, its focus on broad protocol policy issues has caused key standards to develop beyond its structure. Perhaps the best example of such development outside of the IETF is found in the World Wide Web Consortium (W3C). W3C is self-described as primarily active in "developing protocols and guidelines that ensure long-term growth for the Web."[125]

---

[122] Laura Denardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, Mass.: The MIT Press), 26.
[123] Laura Denardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, Mass.: The MIT Press), 28.
[124] Internet Architecture Board, "A Brief History of Internet Advisory/Activities/Architecture Board," IAB Website, 2011, accessed March 25, 2013, http://www.iab.org/about/history/.
[125] World Wide Web Consortium, "Help and FAQ >> What Does W3C Do?" W3C website, accessed March 25, 2013, http://www.w3.org/Help/#activity.

Tim Berners-Lee, the director of the consortium, first tried to situate the Web and protocol development within the auspices of the IETF. In proposing standards to the IETF, however, he found himself falling into "philosophical rat holes" that delayed the establishment and promulgation of standards for the Web. Berners-Lee wanted first and foremost to promote the Web.[126] As the Web became a commercial space, the lethargic nature of the IETF caused Berners-Lee to partner with MIT to establish the W3C. This action let him retain neutrality over standards decisions by basing Web standards on their usefulness for promoting the Web as opposed to promoting particular commercial interests. His decision also let him avoid the "rat holes" of the IETF's public discussions and mailing lists.

The primary challenges facing the consortium revolve around "finding the minimum agreements, or protocols, everybody would need in order to make the Web work across the Internet." The Consortium is not as inclusive as the IETF; membership "is restricted to organizations (and, in theory, individuals) who are willing to commit to a three-year initial membership, with annual dues ranging from $5000 for non-profits and smaller for-profit organizations to $50,000 for larger corporations."[127] Working on a consensus-based model, the organizers of the consortium lack authoritative powers; W3C can be seen as the venue for decision-making instead of acting as the decision maker itself.[128] Further, the discussions leading to any given standard are not necessarily made public; though consensus-driven, "W3C recommendations that are not seen as being the result of open and inclusive practices may face resistance."[129] Such minimum agreements lack the full weight of a formal standard, and they are not as readily adopted into national standards as ITU 'recommendations', but they tend to enjoy wide adoption. As one of the largest and most influential standards bodies that direct how individuals experience content delivery on a daily basis, W3C's and Berners-Lee's respective vociferous and

---

[126] Tim Berners-Lee with Mark Fischetti, *Weaving the Web: The original design and ultimate destiny of the world wide web* (New York: Harper Business Press, 2000), 60-63.
[127] Harry Hochheiser, "Indirect Threats to Freedom and Privacy: Governance of the Internet and the WWW," *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*, (2000), 252.
[128] Tim Berners-Lee with Mark Fischetti, *Weaving the Web: The original design and ultimate destiny of the world wide web* (New York: Harper Business Press, 2000), 98.
[129] Harry Hochheiser, "Indirect Threats to Freedom and Privacy: Governance of the Internet and the WWW," *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*, (2000), 252.

prolific opposition to filtering the Web make W3C one of the few Internet governance bodies that publicly and substantively opposes realigning power and control to core network hubs.

International Governance Bodies and Control

While the ITU's bureaucratic processes limit who can, and does, participate in its operations, the organization does include a study group dedicated to deep packet inspection. Q17/13 was tasked to study packet forwarding and deep packet inspection for "multiple services in packet-based networks and N[ext] G[eneration] N[etwork] environments." The group focused on "the functionalities of deep packet inspection and multi-service (e.g. IPTV/VoIP) aware identification, lookup, filtering, forwarding and queuing, multi-service multicast and associated MIBs (management information base) in packet-based networks and NGN environment."[130] With an emphasis on managing bandwidth efficiently to ensure high levels of service for time- and loss-sensitive data traffic, the group generated recommendations about the requirements, architectures, mechanisms, and functionalities of instantiating DPI equipment within telecommunication networks. Any subsequent ITU ratifications related to DPI may have limited effects if nation-states and national institutions have already established legal standards for monitoring and mediating data flows using DPI. In short, ITU's practical influence in guiding nation-state or corporate actors' actions may be limited, though its decisions concerning how DPI could be used may give rhetorical or political cover to justify already existing or proposed uses of the technology.

The more inclusive IETF has been ambiguous in its formal stance towards Internet surveillance. In examining IETF RFCs, we see that RFC 3360, "Inappropriate TCP Resets Considered Harmful," pre-empted particular uses of deep packet inspection technologies by Internet service providers. This informational RFC argues that inappropriately severing a TCP connection with a RST packet "is not conformant with TCP standards, and is an inappropriate overloading of the semantics of the TCP reset."[131]

---

[130] ITU, "Question 17/13 – Packet forwarding and deep packet inspection for multiple services in packet-based networks and NGN environment," ITU website, last modified February 6, 2009, accessed August 23, 2012, http://www.itu.int/ITU-T/studygroups/com13/sg13-q17.html.

[131] Sarah Floyd, "RFC 3360: Inappropriate TCP Resets Considered Harmful," IETF, August, 2002, accessed March 25, 2013, http://www.ietf.org/rfc/rfc3360.txt?number=3360.

RFC 793, which discloses the specifications for TCP, maintains that RST should be used only as a flag where "a segment arrives which apparently is not intended for the current connection. **A reset must not be sent if it is not clear that this is the case**."[132] DPI equipment has been used to modify users' data packets to insert RST flags for peer-to-peer related data traffic, the result of which is to terminate the sharing of data between clients.

RFC 3724, which was propagated before DPI became a feature in major telecommunications networks, addressed arguments in favor of network interruption of data packets for security reasons. This RFC maintained that end-based processes can be deployed and invoked to assure authenticity of the ends. The RFC's authors warned that ISPs have economic motivations to differentiate services for their customers and that security may be one differentiated service offering. Regardless of how security is assured, – either by end-points or the core of the network – the authors insisted on preserving "[e]nd user choice and empowerment, integrity of service, support for trust, and "good network citizen behavior" …. Any proposal to incorporate services in the network should be weighed against these principles before proceeding."[133] Security and differentiated services that are made possible by enhanced network control should not sacrifice core principles and values associated with the Internet's path dependency.

The issue of surveillance protocols, in particular, has arisen within the IETF, but a standard has not been reached. In 1999, the IETF began debating whether lawful intercept functionality should be integrated into standards development, with the identified key questions being:

1. Should the IETF develop new protocols or modify existing protocols to support mechanisms whose primary purpose is to support wiretapping or other law enforcement activities?

---

[132] Information Sciences Institute (Jon Postel, ed.), "RFC 793: Transmission Control Protocol DARPA Internet Program Protocol Specification," IETF, September 1981, accessed March 25, 2013, http://www.ietf.org/rfc/rfc0793.txt. Emphasis added.

[133] J. Kempf and R. Austein (eds.). "RFC 3724: The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture," IETF, March 2004, accessed March 25, 2013, http://www.ietf.org/rfc/rfc3724.txt, 10.

2. What should the IETF's position be on informational documents to explain how to perform message or data-stream interception without protocol modifications.[134]

The result of the subsequent far-reaching debate, however, was non-conclusive. As a result, "the issue apparently died with the determination that the IETF neither supported nor opposed implementing a surveillance standard."[135] The decision was, in effect, not to make a decision.[136]

Ultimately, the IETF relies on the openness of its standards-setting process, which is accompanied by a transparent protocol development corrections process, to attract legitimacy in the eyes of Internet developers around the world. Importantly, while RFCs are often highly technical, they can be read and referenced by non-technocrats during policy processes; such citations could suggest that the IETF has some capacity to influence, if not to command, both policy and technical developments. It must be noted, however, that influence may vary across cases if some policy networks and communities take up RFCs more prominently than others. Consequently, the degree of influence that that IETF – or any other standards body – wields may largely correspond with the degree of respect and allegiance that actors hold towards standards organizations.

The W3C is distinguished by its previous efforts to head off regulatory efforts that could mediate content available on the Web. As an example, the Consortium developed the Platform for Internet Content Selection (PICS) to preclude the American government from forcing ISPs to limit information available to students and children. PICS permitted blocking, but by way of filters on client computers instead of on ISPs' network routers.[137] W3C has also tried to enhance privacy expectations and protections. The consortium developed the Platform for Privacy Preferences (P3P) that let website operators make their privacy policy machine-readable. P3P-enabled browsers could be set so that their

---

[134] IESG Secretary, "The IETF's position on technology to support legal intercept," IETF mailing lists, October 11, 1999, accessed March 29, 2013, http://cryptome.org/ietf-snoop.htm.
[135] Charles Vincent and Jean Camp, "Looking to the Internet for models of governance," *Ethics and Information Technology* 6 (2004), 164
[136] It should be noted that, during the November 2013 IETF meeting in Vancouver, the IETF is discussing 'Internet Hardening'. The discussion is meant to examine how to secure Internet communications "in light of pervasive Internet monitoring."
[137] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, Mass.: The MIT Press, 2010), 192-3.

users visited only websites that met their privacy demands.[138] The W3C's valuation of privacy has continued despite P3P's unpopularity: the organization is examining how users are tracked online, has held workshops on the topic, and is trying to help users understand how and why their data is collected and used.[139] In addition, Berners-Lee has publicly spoken against DPI on the basis that "we have to draw the line … between running a successful internet service and looking inside data packets."[140] The rhetorical weight of Berners-Lee, as the 'creator' of the Web, combined with the technical efforts of W3C, indicate the potential for the organization to be appealed to in discussions surrounding DPI, especially as they relate to modifying, filtering, blocking, or modifying content in real time from within the network. Together, then, the three organizations are different on their membership policies – and who can enter the organizations – and their respective positions with regard to surveillance online: the ITU's committee is to suggest how DPI could be used, the IETF has agreed to not discuss systems such as DPI at the level of standards, and the W3C has actively opposed standards, laws, and technologies that would encourage the mediation or surveillance of Web content.

How International Governance Could Explain Deep Packet Inspection

To some extent, each of these organizations is involved in drafting and promoting standards that can subsequently direct how online communications will function. By merit of their routine operations, each organization is 'institutionalized', insofar as the parties are "involved in regular interactions and accept certain norms, conventions, and explicitly formulated rules governing their interaction, and that these rules can be enforced."[141] It is within these institutions that "claimants attempt to resolve appropriation conflicts through collective action."[142] Such appropriations need not focus purely on material goods; they can also focus on capturing or assigning status or power to

---

[138] Lorrie Faith Cranor, *Web Privacy and P3P* (Sebastopol, CA: O'Reilly & Associates Inc, 2002).
[139] See: World Wide Web Consortium, "Privacy Activity" W3C website, accessed March 25, 2013, http://www.w3.org/Privacy/.
[140] Tom Espiner, "Berners-Lee says no to internet 'snooping'," *ZDnet UK,* March 11, 2009, accessed March 25, 2013, http://www.zdnet.co.uk/news/security-management/2009/03/11/berners-lee-says-no-to-internet-snooping-39625971/.
[141] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, Mass.: The MIT Press, 2010), 46.
[142] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, Mass.: The MIT Press, 2010), 63.

particular agents or actors by way of establishing particular digital standards or protocols. The history of each of these organizations has established particular nexuses of power, insofar as certain decision makers – often, technical elites – are invested in advancing their preferred means of encapsulating, transmitting, or mediating data. The more successful actors' decisions, to date, have established particular power relations between those who compose, transmit, and receive data.

Though the degree of non-state actor involvement may be higher with regard to Internet institutions than entrenched, state dominated institutions that predate the Internet, these Internet institutions retain 'normal' institutional characteristics. The actors that participate in these institutions form epistemic communities that are, themselves, differentially situated in international policy regimes. Such communities have members that are "united in rejecting some alterative vision of the world, and this common attitude eases coordination problems…There is substantial latitude among members of the community about the precise right answer, but there are strong common aversions."[143] Such aversions often relate to domestic politics, insofar as similar domestic policy or regulatory pressures can direct how epistemic communities realize problems and solutions.

These communities are often composed of elites who are inside and outside of formal political channels; these communities neither need to be large[144] or made up of predominantly international actors. Further, these communities do not necessarily all work within the same specific institution that dominates a policy issue: the regimes of policy making are complex, often nested or partially overlapping, and rarely hierarchically ordered.[145] Telecommunications standards, as an example, reveal a host of different standards organizations that are invested in establishing how different kinds of content are communicated and standardized, often using significantly different governance and enforcement pressures. This complexity means that there are "openings

---

[143] Peter F. Cowhey, "The International Telecommunications Regime: The Political Roots of Regimes for High Technology," *International Organization* 44(2) (1990), 172-3.
[144] Emanuel Alder and Peter M. Haas, "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program," *International Organization* 46(1) (1992), 380.
[145] Karen J. Alter and Sophie Meunier, "The Politics of International Regime Complexity," *Perspectives on Politics* 7(1) (2009), 13.

for non-state actors to influence outcomes"[146] though the ability for non-state and state actors alike to reorder global regimes is "most likely to occur when new coalitions successfully challenge domestic regulatory bargains in countries with significant impacts on the world market."[147] Consequently, the capability for epistemic communities to influence policy regimes depends on domestic political arrangements to maximally influence international governance actions.

The negotiations that occur within international standards bodies constitute a form of governance on the basis that each body places "emphasis on the multiplicity of the actors." Given this multiplicity, the organizations are involved in the "management of international affairs not as an inter-state activity, but as a negotiation/interaction process of heterogeneous participants."[148] Such negotiations mean that, while states may be privileged in the ITU, in each venue state, corporate, and other private (elite) actors can come to the table to establish consensus concerning next-generation systems. Parties that are often involved in setting standards include "firms, activist organizations, and other non-state groups operating at both the domestic and international levels",[149] who may see international governance organizations as spaces to establish, reify, or oppose domestic-minded policies, issues, and positions. As venues, however, these organizations can act as agents of both coercive and voluntary transfer – or imposition – of standards policy.[150] ITU decisions can be used as a cudgel to 'encourage' all vendors to incorporate certain practices into their devices, whereas some IETF and W3C specifications – with their respective inability to levy any kind of formal punishment for non-adherence to standards – may be considered more voluntary in nature.

However, while these organizations are open to participants, almost all involved in the standards-setting process are elites. Many of the issues they address are new and

---

[146] Karen J. Alter and Sophie Meunier, "The Politics of International Regime Complexity," *Perspectives on Politics* 7(1) (2009), 21-2.
[147] Peter F. Cowhey, "The International Telecommunications Regime: The Political Roots of Regimes for High Technology," *International Organization* 44(2) (1990), 171.
[148] Marie-Claude Smouts, "The proper use of governance in international relations," *International Social Science Journal* 50(155) (1998), 84.
[149] Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organizations* 54(3) (2000), 429-430.
[150] David P. Dolowitz and David March, "Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making, *Governance: An International Journal of Policy and Administration* 13(1) (2000), 12.

highly complex or theoretical. In light of this situation, and the fact that underlying problems may be poorly understood, states can delegate authority to a central party (for example, a court or international organization) to address the issues[151] and only intercede when the politics or policies that the organization is addressing are clearly relevant for domestic or transnational issues. However, intervening is not guaranteed to elicit a standard, though even the proposition of, or opposition to, a standard can be sufficient to give 'cover' to actors who want to comply with, or advocate against, a proposed domestic policy position.

The nature of protocol standards-setting can be difficult to situate; while some scholars assert that code is law and that standards bodies now function as legislative bodies, such statements focus on the *functional* as opposed to the *legal* definitions of code and of national democratic legislatures. To be more precise, organizations and institutions that establish 'hard law' undertake "legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations) and that delegate authority for interpreting and implementing the law."[152] States are often party to such laws, in the international domain, and explicitly in terms of passing domestic legislation. 'Soft law', in contrast, is generally characterized by the lack of such legal arguments. This simultaneously increases the number of organizations that can 'pass' soft laws while reducing the necessarily democratic conditions of legitimacy that is associated with national, constitutionally backed law making or ordering. However, even the lack of 'hard' agreements can lead to significant long-term effects, insofar as soft law commits organizations to particular forms of discourse and procedure. In the case of Internet governance organizations, such laws can commit towards paths that dictate or 'strongly recommend' how data is migrated between locations. Moreover, while 'soft' lawmaking might lack formal democratic legitimacy the nature of taking part in decisions may be more or less open. As discussed previously there is a gradient of participatory 'openness' between the ITU, IETF, and W3C, with the ITU and W3C being the least open and IETF as welcoming to any interested (expert) parties.

---

[151] Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organizations* 54(3) (2000), 441.
[152] Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organizations* 54(3) (2000), 421.

Though the decisions made by international organizations can be understood as soft law, such law doesn't fully capture the potential means by which organizations can entrench or disrupt existing technological status quos. In short: if these organizations don't want 'the law' (i.e. code and protocol) to change then they could try and resist changes by refusing to consent to their passage (as was the case with the IETF and wiretapping protocols). Alternatively, however, these organizations could be used to 'launder' policies meant to either adjust or lend credence to specific actors' efforts to modify existing Internetworking principles or standards (as was the case with the IETF and wiretapping protocols). So, the very act of generating debate may offer one degree of 'soft law'; while standards debates alone "cannot be invoked as law, they support a similar normative discourse."[153] Though it is often 'activists' that use soft law as a mechanism to "expose gaps between international commitment and actual government conduct," this activity does not preclude corporate or government interests from similarly using soft law for rhetorical and political purposes.

The very effort to insulate policies vis-à-vis Internet standards can be defined as a type of policy laundering, or the process in which "policy-makers make use of other jurisdictions to further their goals, and in doing so they circumvent national deliberation processes."[154] While such laundering is often associated with the actions of nation-states, policy entrepreneurs, such as corporations, advocacy associations or groups, and well-resourced individuals, might similarly try to establish international 'consensus' on an issue before (re)introducing the issue 'at home.' The worry that standards bodies could be used for policy laundering increases as public and private interests more routinely recognize standards organizations as important for legitimizing these bodies' own practices. As Drake writes,

> The increasing importance of standards has raised the stakes for major industry players. Accordingly, many of these companies have become more aggressive in attempting to control the process in order to push their preferred solutions … in

[153] Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organizations* 54(3) (2000), 452.
[154] Ian Hosein and Johan Eriksson, "International policy dynamics and the regulation of dataflows: bypassing domestic restrictions," in *International Relations and Security in the Digital Age*, eds. Johan Eriksson and Giampiero Giacomello (New York: Routledge, 2007), 162.

> the view of some observers, even "native" Internet standards bodies like the IETF and W3C, which are often depicted as models of distributed yet efficient democratic decision making, have been increasingly impacted by pressure from major firms in recent years.[155]

Of course, the specific tactics of laundering – and efforts that standards bodies can exercise to resist novel means of acting on Internet data – varies according to the institution's means of distributing power, of making decisions, and resolving disputes. Through the framework of international Internet governance, we might expect to see one of the following situations might unfold. In the first, standards bodies are neither significantly influential in domestic deployments of technologies like DPI, nor are they used to launder or justify domestic practices. If this is the case, it would suggest that domestic drivers are primarily responsible for governing DPI-based decisions, or that sufficient domestic forces have not developed to exercise international influence. Alternately, we might expect that standards bodies could see their standards used as 'weak' soft law, insofar as their standards form an element of a broader strategy to justify or oppose particular technologies or practices. This viewpoint suggests that domestic interests were, at least partially, attentive towards international proposals and suggests further that domestic policies were being justified by internationally-present epistemic communities or those communities' decisions. Finally, we might expect to see standards bodies being used to launder policy and establish 'harder' soft law; that is, domestic agents who outsource policy development to standards bodies and subsequently use standards as a significant factor in their attempts to justify domestic networking practices or processes. This interpretation suggests significant interoperability between domestic and international epistemic communities and indicates the interpenetration of domestic and international policy regimes.

In Chapters Four, Five, and Six, it will be possible to gauge whether standards bodies have played a significant role in what is driving DPI's uses in our case studies. To be clear, driving in this case doesn't necessarily mean justifying the technology or its

---

[155] William J. Drake, "Memo #3: ICT Global Governance and the Public Interest: Infrastructure Issues," for the Social Science Research Council's Research Network on IT and Governance, 2004.

practices; instead, driving here means that the bodies are being used to *oppose* how the technology is being used or deployed. It is possible that the standards bodies have played little or no role in the unfolding of domestic applications of the systems, that their standards are routinely used to justify or oppose the systems like DPI, or that actors in domestic policy communities have used or are thinking of using the international bodies to launder policies. In the latter two situations, standards bodies might be seen as playing a medium to significant role in the politics of deep packet inspection in Canada, the US, and the UK. In contrast, should the first situation more appropriately express the significance of the standards bodies in domestic politics, then their role, in the states under study, may be considered minimal or quite low.

The Politics of Framing

The previous frameworks let us focus on whether technological decisions or Internet governance organizations are principally driving DPI. This section, in contrast, focuses on whether the domestic politics of agenda-setting, problem definition, and framing can be used to explain how domestic actors are responsible for driving DPI's deployment and adoption. To this end, I discuss how policy communities are constituted, how and when policy options are manifest to actors, and how policy actors can be expected to frame issues and engage with one another when placing items on a governmental agenda. Taken together, this section provides the theoretical foundation on which the case studies will be arranged – that is, in the format of policy actors and networks – while still leaving the question of whether these domestic actors and institutions are primarily responsible for driving the politics surrounding deep packet inspection.

Policy Actors, Networks, and Communities

Actors in policy networks and communities contest particular issues and aim to position their problems and solutions as the 'right' way forward. Actors are the individuals, the corporations, or other unique parties invested in any particular issue and are often drawn together in policy networks. Such networks bring together actors who are assumed to participate "to further their own ends" which are "seen as essentially material and

'objectively recognizable' from outside the network."[156] Linked to their material interests is some kind of epistemic awareness of the issue, at least as it relates to the actors' own interests. In the case of Internet policy, parties may be materially interested in who provides Internet service, who provides various Internet communications protocols, who produces content that is sent across ISP networks, or who communicates using data networks for public or private purposes. In effect, policy networks "refer to dependency relations that emerge between both organizations and individuals who are in frequent contact with one another in particular policy arenas."[157] Given the breadth of potential issues, Internet-based policy networks can encompass a broad set of actors.[158]

Actors do not always act independently, however, and often tend to situate themselves amongst policy communities. These communities are composed of actors who share common policy focuses and knowledge; networks link the disparate communities to give shape to the broader group of actors invested in any particular policy area. More specifically, policy communities include actors that share "a commonly understood belief system, code of conduct, and established pattern of behavior."[159] While various communities may be interested in Internet-related issues, such as copyright, accessibility, or security and privacy, and so forth, it is via the policy network that they come together and engage with one another before the public and regulators.

These communities will often hold specialist knowledge concerning what the policy network as a whole is addressing, with different actors in the community possessing varying kinds or degrees of knowledge and holding (variable degrees of) material interest in the issue. While the communities as a whole may possess high levels of knowledge about how their members would be materially affected by regulatory changes, these communities may or may not hold common discursive positions; simply

---

[156] Michael Howlett and M. Ramesh, *Studying Public Policy: Policy Cycles and Policy Subsystems* (Toronto: Oxford University Press, 2003), 151.
[157] Michael M. Atkinson and William D. Coleman, "Policy Networks, Policy Communities and the Problems of Governance," *Governance: An International Journal of Policy and Administration* 5(2) (1992), 157.
[158] Mueller, in *Networks and States: The Global Politics of Internet Goverance*, recognizes that intellectual property, critical Internet resources, international trade regimes, and 'cybersecurity' as just some of the core issues within the domain of Internet governance.
[159] Pross, (1986), 98, quoted in Michael M. Atkinson and William D. Coleman, "Policy Networks, Policy Communities and the Problems of Governance," *Governance: An International Journal of Policy and Administration* 5(2) (1992), 158.

because two actors are members of the copyright community, for example, does not mean that they agree on the solution of copyright problems or have a common understanding of what copyright 'means'. Instead, co-membership means just that members generally agree with the basic terms and principles needed to engage in an expert-level debate about copyright itself. In essence, though the communities possess a common 'short hand,' their "assumption of mutual understanding, however widespread, is often false, concealing discursive complexity. Even when actors share a specific set of storylines, they might interpret the meaning of those storylines very differently."[160] This falsity refers to a mistaken belief that parties hold commonly derived positions: while all parties might think that protecting copyright is important, the motives, principles, and normative underpinnings of this position might vary significantly between 'common' parties. Moreover, the 'solutions' to solving the 'problem(s)' of protecting copyright might vary significantly. The degree to which storyline interpretation varies can be used to gauge the relative consistency or discursive stability of the community and its members.

In aggregate, at least three divisions of agency exist that we must remain mindful of when exploring framing and agenda setting: actors, their communities, and the policy networks they debate within. However, when a group of communities disagree with one another, each may contest the basic terms used by other actors in the policy network. These differences can pit opposing communities – and their associated actors – against one another as they try to frame and shape issues to the relevant regulator or public policy outlet. Moreover, these communities can perceive problems *and* solutions differently; often, they may have a 'solution' in pocket and seek to fit it to a problem. In effect, what constitutes a problem often depends on a party's role in a policy network: it is when there is a "mismatch between the observed conditions and one's conception of an ideal state" that a problem manifests.[161] Solutions to problems may often pre-date the 'problem' itself, insofar as actors may try to apply "sufficiently similar" solutions to the problem in an effort to impose their preferred mechanisms for policy resolution onto a policy network. Alternately, communities or individual actors may be emotionally attached to

---

[160] Maarten Hajer and Wytske Versteeg, "A decade of discourse of environmental politics: Achievements, challenges, and perspectives," *Journal of Environmental Policy & Planning* 7(3) (2006), 177.
[161] John W. Kingdon, *Agendas, Alternatives, and Public Policies (Second Edition)* (Toronto: Longman, 2003), 110.

solutions because the solution resonates positively with a political ideology or outlook. Where considerable effort has already been invested in the solution – at a rhetorical, technical, or political level – then the sunk costs of those investment(s) might enjoin actors to push for their solution, even if it doesn't fit the problem particularly well. [162]

In the event of significant contestations over whether a problem exists or whether proposed solutions are appropriate, an unexpected policy window may open. New or unexpected policy entrepreneurs can attempt to take advantage of such windows by offering their own definitions of problems and solutions and attempting to marshal political interests to ensure the issue is framed in accordance with the new entrant's interests or positions. In effect, if the communities in a network strongly dispute one another's framing of an issue and, by extension, regulatory or political aims, space can open for new policy entrants to try and (re)shape issues on the network's agenda. This behavior often threatens the basic terms or policy understandings held by long-standing members of the particular policy network and can provoke strong reaction for not just members of the most directly affected network. Since changes in one policy network can have consequences for others, it is possible that policy entrepreneurs can unexpectedly invite opposition from those outside of the policy network that is being 'reformed'.[163]

In the face of the unexpected opening of a window, path-dependent technical systems may suddenly come to a turning point, where political actions may decide the next turn, or previously settled understandings of international standards might be re-opened to national debate. In essence, unexpected windows can potentially disrupt settled networks and their associated communities and can introduce unexpected actors to the policy network and its discourse. Given the range of political, social, and economic attention given to deep packet inspection – as noted in Chapter Two – the politics of DPI themselves may indicate opportunities to 'solve' other policy problems.

---

[162] Bryan D. Jones and Frank R. Baumgartner, *The Politics of Attention: How Government Prioritizes Problem* (Chicago: The University of Chicago Press, 2005), 47-8.
[163] Michael M. Atkinson and William D. Coleman, "Policy Networks, Policy Communities and the Problems of Governance," *Governance: An International Journal of Policy and Administration* 5(2) (1992), 174.

The Strategic Dimensions of Agenda-Setting and Policy Framing

Taking advantage of policy windows is not a simple, or fully rational, process. Whereas a rationalist model might map the agenda-setting processes that occur in such windows linearly, from problem definition, to solution identification, to political acceptance and legitimation of problems, this linear progress is limited in its practical applicability. Instead, we can capture the constellation of actors and communities, and their respective behaviors, through a 'multiple streams framework' that "points to the relatively independent problem, policy, and political streams within a policy process, and explains policy change by the exploitations of windows of opportunity by policy opponents or policy entrepreneurs."[164] This multiple streams framework is perhaps most useful to explain policies and policy events as something other than linear; solutions proposed by political actors may precede problems, policies may emerge that only loosely address the problem, and problems may arise without either a policy community or political inclination to address them. So, where we see any of these streams open, we can evaluate which 'stage' problems, policies, or politics came 'first', and thus better understand the nature of a policy process itself.

The problem stream predominantly involves understanding variations from normal practices and assessing the magnitude of changes based on existing indicators. With this understanding, actors can determine whether they have found, or can argue for, a new or recontextualized problem. When an unsteady state exists — when, for example, unexpected policy windows open — actors can link policy events with highly symbolic behaviors, such as violations of principles that infringe on sacred values or stated and respected principles, to frame and promote the problem in question. Success in focusing attention will often depend on whether efforts correlate with a focusing event. Such events are "sudden, relatively rare, can be reasonably defined as harmful or revealing the possibility of potentially greater future harms, inflicts harms, or suggests potential harms that are or could be concentrated on a definable areas of community of interest, and *that*

[164] Sander V. Meijerink, "Understanding policy stability and change: The interplay of advocacy coalitions and epistemic communities, windows of opportunity, and Dutch coastal flooding policy 1945-2003," *Journal of European Public Policy* 12(6) (2005), 1061.

is known to policy makers and the public virtually simultaneously."[165] Where a focusing event is missing, it may be challenging to contest the validity of existing policy indicators, responses, or domains of issue contestations. Such challenges arise because focusing events can disrupt the normal conditions of issue framing. So, in the event of a focusing event, the range of what can and cannot be thought can change and, as a result, the range of policy options and prospective policy outcomes can shift.[166]

The policy stream is concerned with the composition of policy communities and how they advance their interests by advocating their preferred solutions. If the policy communities are fragmented, then policy entrepreneurs may emerge to "promote their values, or affect the shape of public policy."[167] For actors to successfully advance their solutions, the individual or group must successfully frame the issue at hand. In highly established and stable environments, existing actors may claim that the issue is accessible only to 'experts' and thus limit who can try to shape the dimensions of the issue; this delimitation narrows possible solutions that might be taken up. So, for an entrepreneur to be successful in changing the dimensions of the issue and its framing, they might make claims concerning a policy's failure "in an attempt to expand an issue to a broader audience" because such framing "leads to more negative assessments of current policy, thereby creating pressure on the dominant policy community or policy monopoly to open up policy making and accept change."[168] Regardless of whether or not a long-term policy actor or an entrepreneur is attempting to frame any issue for the agenda, they have to consider the relationship between proposed policy actions or solutions and the population(s) that they would affect. Specifically, "[s]ocial constructions of target populations become important in the policy effectiveness calculus because elected officials have to pay attention to the logical connection between the target group and the goals that might be achieved."[169]

---

[165] Thomas A. Birkland, *After Disaster: Agenda Setting, Public Policy, and Focusing Events* (Washington, D.C.: Georgetown University Press, 1997), 22. Emphasis added.
[166] Maarten Hajer and Wytske Versteeg, "A decade of discourse of environmental politics: Achievements, challenges, and perspectives," *Journal of Environmental Policy & Planning* 7(3) (2006), 178.
[167] John W. Kingdon, *Agendas, Alternatives, and Public Policies (Second Edition)* (Toronto: Longman, 2003), 123.
[168] Thomas A. Birkland, "Focusing Events, Mobilization, and Agenda Setting," *Journal of Public Policy* 18(1) (1998), 55.
[169] Anne Schneider and Helen Ingram, "Social Construction of Target Populations: Implications for Politics and Policy," *The American Political Science Review* 87(2) (1995), 336.

The third, explicitly political, stream of the agenda-setting process can be particularly important for entrepreneurs to develop and grow their base. Entrepreneurial advocacy bodies may be most successful in establishing external pressures upon politicians, especially in the absence of established lobbyists, though officials overseeing policy subdomains may experience pressures from actors who are typically most invested in the overseen domain. Where parties are entrenched, we might expect such parties to try and exclude new entrants from being integrated into the policy process. Such refutations may see established, long-term actors refusing to collaborate or bargain with new entrants or establishing pseudo-positions that give the appearance of bargaining without moving away from key principles, policy positions, or other elements central to the established actors' bargaining position; or they may rely on political procedures to baffle and exclude new entrants.

Though policy advocates position themselves in relation to one another's framings, the advocates must be mindful of the reality of politics. Such officials "care about outcomes and fear widespread public reaction against ineffective policy, lack of attention to important problems, and too much favoritism to special interests. They may confront these contradictions through strenuous efforts to keep such issues off the agenda, or they may manipulate the images of target groups in an effort to change their social construction."[170] Consequently, framing policy depends on an actor not just successfully setting the discursive frame for the issue they are advocating for or against; framing policy also depends on comprehensive attention to the political interests of government actors. Government cannot be seen as a 'neutral' stage on which any framing can take place, but as a charged domain wherein some policies are bound to fail unless they are expressed in a manner amenable to the politics of the day.

In aggregate, the multiple streams framework helps us understand and explain how issues arise, or are shaped, by the policy advocates in policy networks: do advocates appear, and act, in one stream or another, and what is their relative effectiveness in choosing the stream they do over other policy actors? Moreover, the solutions that actors pose do not necessarily develop only when a problem arises; solutions, like problem

---

[170] Anne Schneider and Helen Ingram, "Social Construction of Target Populations: Implications for Politics and Policy," *The American Political Science Review* 87(2) (1995), 338.

definitions, can float around a policy community and be grasped and applied only when an appropriate policy window opens.

How Domestic Framing Could Explain Deep Packet Inspection

In general, we might understand framing as shaping the potential range of policy problems, options, alternatives, and solutions concerning any given issue. While there are sometimes significant variations in how problems are addressed, "decision makers lean heavily on preexisting policy frameworks, adjusting only at the margins to accommodate distinctive new situations."[171] Actors invested in framing issues are often motivated to express how a given policy issue is, or is not, experiencing a policy failure and deserves a non-incrementalist response because such a response might establish significantly different policy responses, responses that an incrementalist approach may bar. Ultimately, this framework lets us focus on domestic actors and explain how they might be driving the deployment and adoption of DPI.

Even in the face of a 'settled' issue, the groundings of any given policy remain unstable insofar as they are "constantly the object of political contestation."[172] As an example, it might be a settled policy that citizens should have access to broadband communications networks, but the reasons for such access might remain contested. Is access primarily meant to meet constitutional rights (speech, association) requirements? To ensure strong economic growth? To provide affordable access to digitally-mediated healthcare services? Some other ultimate gain? The choice of one primary driver over others doesn't necessarily foreclose other principles from being linked to a policy initiative, but the primacy of any particular principle can reorient the discourse of the policy network — which actors are predominant, and what the tactics and framings that actors might use with government officials and politicians. When powerful actors are threatened — perhaps by another party seeking to situate an alternate principle as a primary driver of a policy — those actors "will try to override developments at the level of discourse" often by cloaking themselves and their interests in the language(s) of their

---

[171] Paul Pierson, "When Effect Becomes Cause: Policy Feedback and Policy Change," *World Politics* 45(1) (1993), 612-3.
[172] Maarten Hajer and Wytske Versteeg, "A decade of discourse of environmental politics: Achievements, challenges, and perspectives," *Journal of Environmental Policy & Planning* 7(3) (2006), 177.

policy competitors.[173] So a party interested in securitization might, faced with a situation where free speech is becoming a primary policy drive, express their 'solution' as one that maximally *secures* free speech.

All efforts to frame particular policies depend on constructing the policy's target populations. The social construction of these populations "refers to the cultural characteristics or popular images of the persons or groups whose behaviour and well-being are affected by public policy. These characterizations are normative and evaluative, portraying groups in positive or negative terms through symbolic language, metaphor, and stories."[174] Policy actors who are most successful in such constructions will discursively frame the populations so the frame "may become so widely shared that they are extremely difficult to refute even by the small number of persons who might disagree with them."[175] Effectively establishing such characterizations can be important; by characterizing 'who' and 'what' a target population 'is' certain policy options may become immediately apparent or foreclosed. So, if a group of policy entrepreneurs is seen as representing 'bandwidth hogs' who 'pirate' content from the internet using 'bad' or 'dirty' applications, officials may adopt retributive policy proscriptions. However, if the same population is seen as 'early adopters' who embrace 'next generation' sharing economies using 'beta version' software that could subsequently drive an 'information economy', then alternate policy options might seem more appropriate. In effect, framing communities is often about identifying victims and culprits with 'solutions' falling out of these characterizations.

That the framing process is often competitive means that different parties try to compromise their policy opponents' language. Parties that more successfully frame issues may see their problems, or solutions, be taken up by the government's agenda: as a result, successfully framing issues can lead to policy or legislative decisions that affirm preferred problems and solutions, while excluding those that threaten an actor's own agenda.

---

[173] Maarten Hajer and Wytske Versteeg, "A decade of discourse of environmental politics: Achievements, challenges, and perspectives," *Journal of Environmental Policy & Planning* 7(3) (2006), 179-80.
[174] Anne Schneider and Helen Ingram, "Social Construction of Target Populations: Implications for Politics and Policy," *The American Political Science Review* 87(2) (1995), 334.
[175] Anne Schneider and Helen Ingram, "Social Construction of Target Populations: Implications for Politics and Policy," *The American Political Science Review* 87(2) (1995), 336.

In a domestic situation, then, we might imagine a series of different manners that explain how and why issues are framed. First, domestic framings of issues and groups, as well as potential policy options that rise to the agenda more generally, might fit within proscribed technical or international governance positions. This stance might indicate a synergy between domestic, technical, and international constituencies. Second, domestic issues might see governments try to excise or shape policy issues, often in opposition to the framing efforts by non-governmental or private bodies'. Governmental agency would significantly repudiate the notion that policy networks are critical in shaping domestic policies; it could also weaken arguments that path dependency or international governance necessarily influence Internet-related policy issues. Finally, we might find that either non-governmental or private bodies predominantly drive domestic applications of deep packet inspection, with government largely drawing from such external bodies of expertise. This situation would confirm the significance of policy networks and also suggest that the government is predominantly a passive receptor of policy from the relevant networks.

How issues are framed domestically will serve to identify commonalities and differences between Canada, the United States, and the United Kingdom. We may find that each jurisdiction has strong general variances in the domestic policy process, which indicates a broader difference in how paths or international governance inflect domestic policies. Alternately, there might be *policy* commonalities that focus on domestic issues that significantly cohere with technological paths; in such instances, though path dependency itself may not principally explain the relevant driver, we might see that 'technical realities' constrain policy problems and solutions. Finally, when comparing across cases, we must pay attention to the important role of international governance insofar as it may indicate whether domestic epistemic communities are reaching out to, or being integrated with, their counterparts globally. Even if these communities are not successful in framing domestic policies, their very existence is significant because it suggests a domestic policy capacity and ability to build a policy community that integrates domestic issues within the global context.

Conclusion

This chapter provided three frameworks that might explain what is driving DPI. The first revolves around technological path dependency. In examining ARPANET, I discussed how decisions and values that guided the research network's development have established paths for the contemporary Internet. Deep packet inspection could rearticulate the power relationships these dependencies established: will the ends continue to be prioritized over the network core, and will a *capacity* to reorient power relations lead to *actual* redistributions of power? This framework lets us explain whether DPI actually functions as a disruption to Internet systems and whether, if it does represent a disruption, it provokes a minor or significant reorientation of the current technological path.

The second framework revolves around the role of international Internet governance bodies. Here I raised questions about the effective influence that these bodies could have on the framing and deployment of deep packet inspection devices. Do they have any influence whatsoever and, if so, do their actions and standards function as either 'weak' or 'hard' soft law? This framework makes it possible to explain the relative role of these institutions that some have been argued as being the governance institutions of the contemporary Internet and data protocols: do these institutions exercise much 'governance' in terms of deep packet inspection?

The third framework emphasizes the importance of domestic policy networks in mobilizing and responding to material technical changes in digital networks. Here, I am interested in explaining whether domestic actors are significantly constrained by path determinacy or international governance decisions. Alternately, it is possible that, despite influences from earlier paths or international decisions, domestic governments are driving attempts to frame DPI or that, in contrast, non-government (e.g. corporate or civil libertarian) groups are most active in framing issues for government.

Though each framework is proposed in discrete terms, it is entirely possible that in any given case a mix of the frameworks might be present: DPI might be seen as a significant disruption when cast through path dependency but as insufficient to independently modify the totality of the technical infrastructure. It might be that a combination of international governance and domestic politics, in tandem with this (potential) technological disruption provokes *some non-uniform* changes in each case. So,

each framework may differentially explain aspects of the politics of deep packet inspection without any particular framework that explains the full story. Moreover, each of these frameworks enables a comparative policy analysis of how DPI has been adopted in the cases studies; a broader democratic theory will likely be required to capture the normative implications that DPI-based practices have on the character or quality of communications between residents of democratic states.

I now turn to the cases through which I will see how these frameworks play out. Each of the states that I chose for the cases uses a common language, is similarly represented at the ITU, and includes a mature set of networks that could be invested in how DPI is framed and deployed. Similarly, deep packet inspection has been widely deployed in each of these states, though perhaps not for identical purposes. Examining these states will reveal what is driving local deployments of DPI, the roles of technological path dependencies, the influence of international bodies, and the roles of local policy networks. These empirical analyses will be used to ascertain, in Chapter Seven, whether there are commonalities in not just how, but why, the technology is being deployed. Understanding the drivers of DPI is helpful in evaluating the broader significance of the technology, which will be taken up in the final chapter of the dissertation.

Chapter 4: The Canadian Experience

Deep packet inspection first arose as a significant Canadian issue during Canadian Radio-Television Telecommunications Commission (CRTC) regulatory proceedings. What began as a contractual conflict between Bell Canada, one of Canada's largest ISPs, and their wholesale customers over Bell's use of DPI, subsequently spiralled into a more wide-ranging dispute of what was, and wasn't, appropriate monitoring and mediation of Canadians' data traffic. Such disputes were heard at the CRTC, before the Office of the Privacy Commissioner of Canada (OPC), the Canadian Parliament, and in the mass media. This chapter investigates how, and why, DPI emerged as an issue on the Canadian public scene and how policy community framed it as a policy issue.

I begin by investigating the core Canadian policy actors who are interested in DPI and the dimensions of the policy network in order to clarify the general positioning of the actors. Next, I turn to the various issues surrounding DPI: network management, content control, advertising, and national security. When examining each issue, I take up the technical, economic, and political affordances that are relevant to the Canadian situation. Each section includes discussions of the relevant issue, the associated actors, and who appears to have been more or less successful in framing issues or advancing their interests. The chapter concludes by briefly summarizing the key characteristics of the Canadian situation.

Introducing the Actors

On the whole, there has been a relatively small policy network invested in issues surrounding DPI. Over the course of DPI's time as an issue, the actors have coalesced into familiar policy communities. ISPs disagree over how the technology is used to interfere with *one another's* traffic, but they tend to agree about how ISPs should be permitted to use DPI to mediate *their own* subscribers' traffic. Civil society groups have tended to oppose usage of the technology, as have some groups representing rights holders, performers, or others involved in content production or distribution. Equipment vendors have sided with ISPs and insisted on the lawfulness and appropriateness of the practices linked to DPI. Ultimately, only a few government institutions have been drawn into issues directly related to DPI.

Almost all major Canadian ISPs use DPI to some extent, though the full range of uses varies. As a policy community, ISPs can be divided into Incumbent Local Exchange Carriers (ILECs),[176] such as Bell, Rogers, Shaw, Videotron, and Telus, which provide line-sharing services and often are content providers as well, and Competitive Local Exchange Carriers (CLECs), such as Teksavvy and Execulink. ILECs are the owners of core Internet infrastructure. Their line-sharing is a "wholesale service that provides access to the high-frequency band of the unbundled copper local loop"[177] and many CLECs use this service to access the 'last mile' of the Internet infrastructure that is used to transit data traffic between Canadian homes and businesses and CLECs' infrastructures. Many of the CLECs were represented as a uniform group at CRTC hearings by their trade association, the Canadian Association of Internet Providers (CAIP). Though there are disagreements within the community, all members are mindful of how to operate their networks with minimal government regulation.

While ILECs and CLECs are arguably the primary groups with economic interests in the physical and logical configurations of Internet access and provisioning in Canada, other groups have also expressed interest in how networks are managed. Some of these groups include advertisers like the Interactive Advertising Bureau of Canada, Voice over Internet Protocol companies like Skype, search engine providers like Google, as well as a breadth of media groups including the CBC, Independent Film & Television Alliance and the Canadian Film and Television Production Association. These organizations constitute a loose community that shares some common level of understanding of a problem related to DPI; namely its potential to cement control over content distribution on IP networks to telecommunications firms.

Civil society and consumer groups have also been invested in DPI. They have focused on how practices related to the technology could threaten citizens' privacy and potentially discriminate against certain customer and corporate practices. These groups have acted as a relatively cohesive policy community, insofar as they share common principles and tend to assert mutually sympathetic arguments concerning how Canadian

---

[176] Note that ILEC is used in a generic sense to capture both ADSL and Cable Internet companies. Similarly, line-sharing is used to generally describe the sharing of an ILEC's infrastructure with CLECs on both ADSL and Cable Internet networks.

[177] CRTC, "Telecom Regulatory Policy CRTC 2009-34," *CRTC*, 2009, accessed Mary 12, 2013, http://www.crtc.gc.ca/eng/archive/2009/2009-34.htm.

ISPs use, or could use, or should not be permitted to use, DPI. Members of this community include the Canadian Internet Policy and Public Interest Group (CIPPIC) for the Campaign for Democratic Media, and PIAC for Consumer Groups; these groups have seen DPI as (largely) a solution in search of a problem, and a solution that has been responsible for *causing* problems that had not existed previously. Further, CRTC hearings have seen the Council of Canadians with Disabilities and the ARCH Disability Law Center get involved, on the basis that software applications used by the disabled might be disrupted by ISPs' use of DPI. Together, these groups and organizations are concerned about how discrimination against Internet data traffic flows could disadvantage the Canadians whom these organizations represent.

Importantly, the community focused on consumer and civil rights has concentrated on practices related to DPI because, "that ship [i.e. opposition to the technology instead of its related practices] sailed before it was even built; it was already out of the port and off to sea … We never did a full campaign against DPI because once it's in it's impossible to get rid of."[178] Thus, despite the technology often being regarded as "anti-net neutrality," the practices linked to DPI that would infringe on network neutrality have been the primary targets of resistance. Contestations over the technology have been complicated because "DPI's a very hard to catch technology, so it's the same with network trafficking stuff … it's something that's very easy to do surreptitiously and can have very broad impacts."[179]

All of these communities were often identified by the media organizations that covered DPI in Canada. Technical websites such as *Ars Technica*, *DSL Reports*, *Slashdot*, *TorrentFreak*, and *P2PNet* all ran stories that covered issues pertaining to DPI in Canada. Moreover, major dailies such as the *National Post* and *The Globe and Mail* ran premier articles, and there was television coverage when major developments broke. Other international outlets picked up and wrote about the uses and regulations surrounding DPI in Canada.

Many of the primary confrontations between members of this policy network have occurred before the CRTC. As Canada's telecommunications regulator, it is, and

---

[178] Interview with Canadian civil rights advocate, January 30, 2012.
[179] Interview with Canadian consumer advocate, January 30, 2012.

has been, principally responsible for ascertaining when and how DPI can be used, what it can be used for, and the processes that ISPs must adhere to before using the technology in new ways. A series of hearings concerning the uses of DPI have extended over the course of several years at the CRTC. In addition, and as an independent governmental body, the Office of the Privacy Commissioner of Canada (OPC) has been involved in the politics of DPI; it filed a submission in CRTC proceedings and also responded to a complaint, filed by CIPPIC, about ISPs' use of DPI. The OPC has also commissioned and published educational resources about DPI for the public. Finally, though a relatively minor point, a member of a federal political party also expressed some interest regarding DPI-based practices.

Each of these institutions possess a different set of characteristics: the CRTC is a regulatory body, and all communications between it and involved actors are on the public record, whereas the OPC operates as an ombudsperson that releases decisions and incomplete transcripts of investigative processes. As members of the OPC's office have taken other positions across Canada (e.g. the Assistant Commissioner who examined DPI for the federal commissioner is now the Information and Privacy Commissioner of British Columbia), they have broadened awareness of the technology amongst their new offices and have generally been supportive of awareness-raising efforts. Members of Parliament may be sympathetic to particular issues, and their statements and relevant actions are on record, but the full details of who did or didn't lobby, teach, or influence them can be challenging to divine. As a result, the visible processes surrounding how policy communities are invested in the 'politics of DPI' in Canada are evidenced at the CRTC primarily and, to a lesser extent, through the reactions of actors to the decision of the OPC and the statements of politicians.

In summary, a set of divergent policy communities composes the policy network around DPI. ISPs form one group, where most companies want to, at least potentially, use DPI, though there is a core disagreement concerning whether wholesale (i.e. CLEC) customers should be subject to ILEC DPI-driven practices. Media and content generation groups form a second community and have concerns similar to – though not uniform with – those expressed by the consumer groups and CIPPIC. The third group, composed of the consumer and civil rights community, is broadly concerned about the kinds of practices

that DPI enables and, while they are supportive of media groups and CLECs, they adopt positions that would hobble CLECs and ILECs alike. Government organizations, such as the CRTC and the OPC have played critical roles in setting the stages for agendas to be set and issues to be framed. Media have covered the uses of DPI in Canada and, perhaps because of how the public has responded to these stories, politicians have also been involved in framing the technology as threatening to "network neutrality."

The Issues

Actors invested in DPI have generally contested how the technology lets ISPs control their digital networks. In what follows, I identify and discuss how the technology has arisen on Canadian agendas by way of the following issues: network management, content control, advertising, and national security. The issues flowing from DPI often stem from questions of who should be permitted to control the data that flows through ISPs' networks and what the appropriate reasons are to permit or block ISPs from controlling data on their networks.

Network Management

It was predominantly a contractual dispute between ILECs and CLECs that turned DPI into an issue in Canada, and that subsequently led to the government telecommunications regulator to issue a set of decisions concerning how Canadian ISPs could use DPI. In discussing the dispute, I distill the key elements of a set of CRTC proceedings that investigated how the technology was, and could be, used. I also summarize an investigation by the Office of the Privacy Commissioner of Canada into how the technology operates in Canada. Network management has proven to be the most significant policy issue to arise in Canada in relation to DPI, and it has drawn CLECs, ILECs, vendors, civil and consumer advocates, corporations, and other branches of government into the Canadian telecommunications policy network. In what follows, I identify the positions that actors have adopted and the effectiveness of their efforts to frame the issue of network management.

The disputes in Canada began with contestations over Bell's contractual agreements with CLECs in 2008. Bell alleged that CLEC services were generating a significant amount of congestion on the network that they shared with Bell and, as a

result, Bell began "throttling" its wholesale CLEC customers. This throttling delayed the speed at which CLEC subscribers could share data over P2P networks. This delay was identical to the delays that had already been imposed on Bell's retail branch, Sympatico, subscribers. One telecommunications executive described Bell's decision as a "key event in the regulatory space" because the company "told its wholesale ISPs 'as of such and such a date we will be using DPI technologies to manage peer-to-peer traffic.' Didn't really give them a lot of advance notice and kind of appeared to be imposing it on them, and I think that's what really kicked off the regulatory debate."[180] Bell maintained that its decision to throttle, as opposed to terminate, CLECs' service showed a level of restraint that was within the boundaries of the agreements.

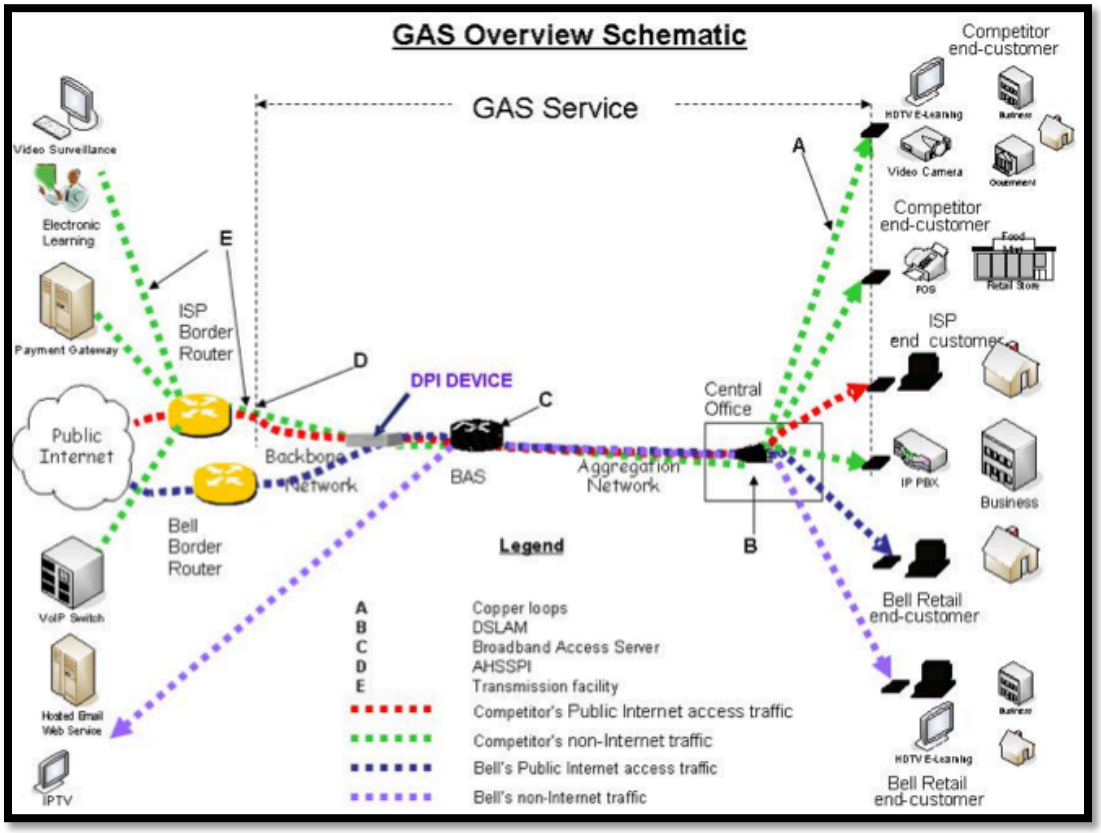


Figure 5: CAIP GAS Overview Schematic[181]

[180] Interview with Canadian ISP executive, January 31, 2012.
[181] CAIP. (2008). "Before the Canadian Radio-television and Telecommunications Commission: Reply of the Canadian Association of Internet Providers," *CRTC*. Published July 23, 2008. Pp. 12.

The arguments of CAIP and the CLECs sought to frame the uses of DPI along three main streams. First, they made a technical argument. Bell's equipment was being inappropriately deployed; rather than positioning the devices close to the 'ends' of the network (either the Digital Subscriber Line Access Multiplier (DSLAM) or Central Office, which are proximate to where Internet connections terminate to subscribers), the equipment was placed beyond the Broadband Aggregation Service (BAS). Figure five provides a depiction of where the appliances were located, in reference to Bell's broader network infrastructure. This positioning meant that the equipment could only be used as a blunt instrument: instead of being able to correct for *local* congestion that might affect subscribers towards the Central Office, Bell established *global* restrictions on network activity to try and address localized congestion issues. Moreover, as bluntly stated by Vaxination Infomatique, "it is impossible to have 100% foolproof way, even with DPI equipment to guess what application protocol is being used in a packet."[182] In line with this critique of DPI equipment, CAIP provided evidence that Bell's use of DPI was inappropriately affecting virtual private networks and other non-P2P data traffic.[183] Consequently, the very capacities of the technology itself were brought into question.

Second, there was a business argument. The stated problem with Bell's approach was that a subscriber of TekSavvy or Execulink was *not* in a direct contractual relationship with Bell. By merit of Bell's ability to rapidly change the terms of how CLECs' networks functioned – and the service provided to their customers – the CLECs could not independently run their own businesses. Consequently, Bell's use of DPI was identified as 'anticompetitive' because competitors that used aspects of Bell's infrastructure could not differentiate their retail service offerings significantly from Bell's own.

Third, there was an argument for *when* DPI could be used. CLECs, generally, wanted the ability to use this technology to mediate their own subscribers' data traffic. Thus, the CLECs sought to differentiate how DPI could be used to affect CLECs that

---

[182] Vaxination Infomatique, "Re: Public Telecom Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet Service Providers – Reference: 8646-C12-200815400," *CRTC*, February 23, 2009, accessed March 21, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029877.pdf.

[183] CRTC, "Telecom Decision CRTC 2008-108," *CRTC*, November 20, 2008, accessed May 12, 2013, http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm.

used an ILEC's line-sharing service and how *all ISPs* could use DPI to affect their own subscribers. These three arguments were applied in both the first and second CRTC proceedings that examined the use of DPI in Canada.

ILECs disputed CAIP's characterization of DPI's usage throughout the CRTC proceeding. Bell maintained that throttling (as opposed to termination of service) indicated a level of restraint and did not constitute unjust discrimination; DPI equipment affected only a specific traffic-type that the company had determined was detrimental to the network's functionality. Moreover, several ILECs noted that application-types were not *prevented* from transmitting or receiving data but that they merely experienced delays in how quickly they received or transmitted data. Further, Bell asserted that undue preference was given to the company's own retail Internet subscribers; Bell Sympatico subscribers experienced the same throttling as the CLECs' subscribers. This set of arguments, combined with the assertion that the congestion was experienced on Bell's network, led the company (and other ILECs) to frame the use of DPI for throttling as an effort to treat *all subscribers* on a common network equally. It was 'bandwidth hogs' using Bell's network that were being prevented from 'slowing down the Internet' for non-hogs. Moreover, Bell firmly insisted that the technology was respectful of subscribers' privacy because the company used DPI only for subscriber and network management purposes. Like Rogers, an incumbent cable-Internet operator,[184] Bell insisted that the technology targeted only specific application types and did not unduly or unnecessarily affect subscribers' data traffic.

Despite the fact that TELUS, another ILEC, did not use DPI, the company agreed with Bell's decisions. TELUS maintained that ILECs should not need to notify wholesale customers' subscribers concerning DPI-related network changes because "[c]ustomer relations matters that involve no network interface changes do not engage the network change notification requirements, and it would be inefficient and unwieldy to create new requirements in this regard." Moreover, the company maintained that Bell's use of DPI did not violate principles of unjust discrimination or unreasonable preference to certain

[184] Rogers, "Canadian Association of Internet Providers (CAIP) - Application requesting certain orders directing Bell Canada to cease and desist from throttling its wholesale ADSL Access Services," *CRTC,* July 3, 2008, accessed March 21, 2012, http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923478.pdf, Pp. 3.

subscribers because it identified the 'threshold question' as "whether two customers receiving the same service are being treated differently. In this case, not only are all [Gateway Access Service] customers being treated the same, but both Bell Canada and its resellers' retail customers are being treated the same."[185]

The ILECs' arguments concerning DPI, in short, revolved around contesting what was 'fair' – cast through the lens of 'hogs' using too much of a common network resource – and was combined with statements concerning what were appropriate contractual interpretations of tariffs. Further, the technologies used to enforce network management were cast as precise: the error-scenarios that were put forward by CLECs (and, ultimately, by other participants in the CRTC proceedings) were cast aside as incorrect. Finally, all ISPs denied using – or intending to use – DPI for advertising purposes and noted that such uses would require significant modifications to their existing network configurations.

DPI equipment vendors supported their ILEC customers in defending the use of DPI to conduct network management practices. The vendors were also keen to prevent either of the CRTC's proceedings from turning into full-blown network neutrality proceedings. Vendors asserted that DPI was needed to identify and manage traffic that obfuscated its nature; non-DPI methods of mediating P2P and other 'problematic' traffic flows were simply ineffective.[186] Juniper Network Inc., one of the vendors, asserted that carriers should be allowed to use whitelisting techniques that, rather than delay some data transmission-types (e.g. P2P traffic), would increase the priority to preferred traffic (e.g. VoIP).[187] Though different uses of DPI were proposed, all vendors agreed that network congestion was an issue and that DPI could help defray the problem for their ISP clients.

---

[185] TELUS, "Part VII application by Canadian Association of Internet Providers (CAIP) requesting that the Commission issue certain orders directing Bell Canada to cease and desist from "throttling" wholesale ADSL services and in particular, the wholesale service known as Gateway Access Service (GAS)," *CRTC*, July 3, 2008, accessed March 24, 2012, http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923480.pdf, Pp. 2.

[186] Arbor Networks, Inc., "From: Kurt Dobbins (kdobbins@arbor.net) on behalf of Arbor Networks, Inc. (Arbor) – Re: 2008-19-2," *CRTC,* February 24, 2009, accessed Mach 23, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1032115.PDF.

[187] Juniper Networks, Inc., "Call for Comments Response – Telecom Public Notice CRTC 2008-19," *CRTC*, February 19, 2009, accessed March 23, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029277.DOC.

PIAC offered direct comments on how ISPs' use of DPI might affect consumers. The organization noted that Bell did not notify its own retail customers of the change in network behaviour, and, in fact, made only a small addition to their Frequently Asked Questions (FAQ) document for wholesale customers. No type of DPI-based throttling existed that PIAC approved of; as they stated in their regulatory filings, PIAC "oppose any throttling whether based on time of day, user, source or destination or application … it offers ISPs an incentive not to upgrade their networks and to increase prices of a captive audience."[188] In the case that the Commission approved DPI's use for traffic management, PIAC insisted that retail and wholesale customers be notified of the technology's usage. PIAC also argued that DPI raised privacy issues on the basis that Bell's equipment associated a subscriber with data traffic; this stance paralleled the argument made by CIPPIC in a separate complaint to the Office of the Privacy Commissioner of Canada.

Additional parties opposed how Bell and other ISPs throttled traffic. Skype, a Voice over Internet Protocol (VoIP) provider, argued that *if* there were genuinely congested links within ISP networks, then the least onerous solution – not the overarching Bell Canada solution – should be adopted.[189] CIPPIC recognized that Internet Traffic Management Practices (ITMPs) were justifiable in limited instances where congestion was occurring and where it had an objectively identified, clear, technical characteristic. Despite this recognition, CIPPIC identified a series of IETF-approved methods to address network capacity overload and relied on technical briefs filed with them, as appendixes, by well known Internet infrastructure experts[190] to argue that IETF proposals, instead of DPI, should be used to address congestion.

---

[188] PIAC, "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers – Comments of the Consumers' Association of Canada, the National Anti-Poverty Organization and the Option consommateurs ("The Consumer Groups")," *CRTC*, February 23, 2009, accessed March 23, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030499.zip.

[189] Skype, "Before the Canadian Radio-television and Telecommunications Commission In the Matter of an Application by Canadian Association of Internet Providers Pursuant to Part VII of the CRTC Telecommunications Rules of Procedure and Sections 7, 24, 25, 32, 36 and 62 of the *Telecommunications Act* Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" Its Wholesale ADSL Access Services," *CRTC*, June 12, 2008, accessed October 3, 2012, http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/920240.PDF.

[190] Experts provided full reports, and included Dr. Andrew Odlyzko, Dr. David Reed, and Bill St. Arnaud.

The Council of Canadians with Disabilities and ARCH Disability Law Center filed comments as well and explicitly noted that the CRTC did "not have the power to approve an ITMP that is contrary to the law," in reference to Canadian disabilities laws. They were concerned that the ISPs might not know what applications that the disabled use, so the ISPs would not add those applications to ISP whitelists. Further, these organizations argued that whitelisting (where certain applications are permitted to receive and transmit traffic without interruption) was an unsuitable means of managing traffic, insofar as there would be many applications used by those who are disabled. They ultimately asserted that "traffic management practice needed to be chosen carefully, used only when there is in fact traffic congestion that could not be solved by reasonable provisioning and that is non-discriminatory."[191] In aggregate, the various citizen and consumer groups questioned whether DPI was a genuine solution to a problem experienced by carriers, or whether DPI itself constituted a problem based on the technology's affordances.

The regulatory proceedings at the CRTC also saw the Office of the Privacy Commissioner of Canada submit a filing that was largely the result of their own independent investigations into DPI. In their investigation, the OPC found that Bell's DPI equipment *was* binding Sympatico users' subscriber identifiers with assigned IP addresses. The company was thus collecting personal information and was required to note this collection on its website; the brevity of the collection of such information did not affect the need to comply with federal law.[192] The OPC was unconvinced that subscribers knew how DPI was used and required greater transparency. The OPC also asserted that Bell could not use existing clauses in Bell's "Internet Service Agreement and the Bell Dial-up Services Agreement" to expand uses of DPI (e.g. for advertising).

---

[191] ARCH, "Telecom Public Notice CRTC 2009-19 – Review of Internet Traffic Management Practices of Internet Service Providers: Oral Presentation," *CRTC*, July 8, 2009, accessed March 23, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241696.PDF.

[192] Specifically, the OPC wrote:

> in the past, this Office has always interpreted the *Act*'s intended use of the verb "collect", within the context of collection of personal information, to describe an act of perceiving that information for any length of time, usually with a view to applying the information to a purpose. The fact that the organization chooses not to retain the information afterwards does not discount the reality of a collection having occurred in the first place.

Bell was not found using DPI for anything but subscriber management functions (e.g. throttling).[193]

Although the OPC rendered a decision concerning DPI, it was the CRTC that functioned as the primary space for contesting how the technology was, and could be, used by Canadian ISPs. While the first proceeding on DPI was brought by CAIP – to try and overturn how Bell applied DPI to the common network – the second was more far-ranging and intended to establish what were fair and unfair 'Internet traffic management practices' (ITMPs). The aim of the CRTC in this second proceeding was not to *authorize* or *ban* any particular technology: it was focused on *management practices*, and DPI was recognized as a potential tool that could facilitate such management. It is in this vein that one government official stated that "[f]rom a technical standpoint, strictly, DPI still has a great benefit … but it's been maligned in the industry and the press as being this terrible thing."[194] Consequently, though it wasn't directly evident from proceeding documents themselves, the CRTC was implicitly attempting to frame the very scope of what constituted 'legitimate' engagement with their questions: they wanted a focused discussion on management practices, and not a wide-ranging set of discussions concerning the theory of network connectivity, end-to-end power relationships, and so forth.

In part to broaden the spectrum of debate beyond just the CRTC, advocates and CLECs sought to introduce DPI – and its associated practices – as an issue to the public. Their actions ultimately led to the tabling of a private member's bill in the House of Commons and to a protest on Parliament Hill. The SaveOurNet coalition drew "some 300 citizens who chanted "Our net is not for sale," and "Whose net? Our net"."[195] The rally was principally organized by Teksavvy (a CLEC), and protestors focused not on the contractual dispute between Bell and CAIP but on broader issues of equality of access, freedom to choose throttled versus non-throttled access, the anticompetitive nature of Bell's actions, and the position that ISPs should not have the right to decide which

---

[193] Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2009-010 – Report on Findings: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection," *OPC,* September 2009, accessed March 27, 2012, http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm.

[194] Interview with a Canadian government official, February 1, 2012.

[195] Leslie Regan Shade, "Public Interest Activism in Canadian ICT Policy: Blowin' in the Policy Winds," *Global Media Journal: Canadian Edition 1(1)* (2008), Pp 114.

Internet-capable applications transfer data faster than others.[196] In effect, the protest covered many of the issues brought up in the CRTC hearings as well as some issues that the CRTC sought to downplay.

Charlie Angus, the NDP's Digital Affairs Critic, introduced a private member's bill to amend the *Telecommunications Act* and "prohibit network operators from engaging in network management practices that favour, degrade or prioritize any content, application or service transmitted over a broadband network based on its source, ownership or destination, subject to certain exceptions." The bill would have forced ISPs to notify subscribers about conditions associated with accessing the Internet. The legislation also would have granted exceptions for prioritizing time-sensitive traffic.[197] Neither the Liberal Party of Canada, nor the Conservative Party of Canada (which formed a minority government at the time), supported the legislation. The bill did not move beyond first reading, though it did lead to a discussion in the House of Commons surrounding network neutrality.[198] One telecommunications executive regarded the shift from the CRTC to Parliament as a distinct problem because members of Parliament "don't care what the answer is; they care about what questions they ask because they might be quoted on what questions they ask. They care about what the other party is doing and how they can blame the other party. They don't care about the actual issues."[199] Ultimately, however, the CRTC and OPC have been the primary governmental bodies that have engaged with the technology and policy network associated with it.

The communities arrayed against the ILECs forced the incumbents such as Shaw and Bell to defend their technological uses of their DPI equipment. These communities were able to press 'simpler' messages to the public that focused on (over) simplistic analogies and public-friendly concepts such as "network neutrality." As noted by one Canadian telecommunications executive, "Net neutrality is very sound bite friendly, whereas network management, you need to take the time to explain why you're doing

---

[196] Peter Nowak, "NDP to introduce 'net neutrality' private member's bill," *CBC News*, May 27, 2008, accessed April 7, 2011, http://www.cbc.ca/news/technology/story/2008/05/27/net-neutrality-ndp.html.
[197] Bill C-552, *An Act to amend the Telecommunications Act (Internet Neutrality)*, 2d sess., 39th Parliament, 2008, http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?billId=3463800&Language=E&Mode=1
[198] Peter Nowak, "Net neutrality bill hits House of Commons," *CBC News*, May 28, 2008, accessed March 20, 2012, http://www.cbc.ca/news/technology/story/2008/05/28/tech-netbill.html.
[199] Interview with a Canadian telecommunications executive, January 31, 2012.

something."[200] Another executive raised concerns about the very concept of network neutrality, saying "From a corporate perspective, I think what scares all carriers about network neutrality-type rhetoric is that they may actually lose the ability to control how they manage their networks when it comes to public Internet traffic."[201] Ultimately, however, the "management" functions of DPI were authorized by the CRTC's ITMP decision, which suggests that ILECs and CLECs successfully kept the focus on specific practices associated with DPI and avoided being drawn into more philosophical battles around the concept of network neutrality.

Who most successfully advanced their framing of DPI to the CRTC and OPC's agendas for existent and future uses of DPI varied. The CRTC's decision that regulated how the technology could be used and the OPC's findings that followed from CIPPIC's complaints caused few changes in how ISPs were using the technology. First, in terms of the contractual disputes between ILECs and CLECs, ILECs were largely successful because, while ILECs must provide greater notice to CLECs than historically offered, the modifications of service could still occur. The 'anticompetitive' framing of DPI by CLECs failed to take hold. Second, while the CRTC decisions forced ISPs to reveal to customers what, and how, technical management systems affected certain protocols, those same customers were not necessarily given grounds to protest or oppose new, or more onerous, management practices unless those practices degraded communications to the point they were effectively disrupted. Thus, advocates were (at best) successful in advocating for greater consumer transparency. Third, the CRTC asserted that ISPs could not mediate data flows to the extent that services or content were noticeably degraded. Arguably all parties could, in principle, accept this finding although they strongly disagreed during and after the decision about what constituted a noticeable degradation of service. Without clarity concerning how, or when, to bring complaints, citizen and consumer groups were left without clear guidance for when, or how, to bring a complaint: this lack of guidance hindered any ability to clearly identify when or if an ISP was breaking the CRTC's rules.

---

[200] Interview with a Canadian telecommunications executive, January 31, 2012.
[201] Interview with a Canadian telecommunications executive, January 31, 2012.

Insofar as one Canadian expert defined successful agenda setting as advancing "whatever position is most advantageous to us in the regulatory sphere and the policy sphere"[202] and another as "successful if at the end of the day you get what you want,"[203] then vendors and ISPs were certainly successful in securing current uses of the technology. In the case of the CRTC's decision, one telecommunication executive explained that "there was a lot of head-scratching after the decisions because the existing throttling practices that went into the proceeding, came out of the proceeding unscathed without a word said about them! The people who were fighting against them must've kind of said: "what just happened?""[204] Another executive, while recognizing that advocates were successful in swaying both CRTC commissioners and federal politicians, ultimately concluded that "the policy framework that came out was actually a fair decision. I mean, it's not something that sets rules and prevents network operators from managing their networks at all."[205] An interviewed journalist held a similar view as the first executive, saying "telcos were successful because it's still happening now," though they admitted that some degree of success was enjoyed by all members of the policy network.[206]

In terms of practices not yet implemented by Canadian ISPs, advocates successfully placed privacy-related issues on the agenda in that ISPs were prohibited from introducing certain practices without prior governmental approval. One advocate saw the advocacy work as successful because practices like behavioral advertising and 'privacy invasive' uses of the technology were foreclosed. As this advocate said, "It seems like Bell really wasn't ready for that attack and they fumbled around in the hearing and weren't quite clear if they were or weren't getting subscriber details in their machine even temporarily. And so the Commission got the heebee-jeebees and just said that looks like a privacy violation and you will not use it for marketing purposes, which is our main concern, not so much for its use for security, more for marketing preferences."[207] In contrast, another said DPI is "a privacy invading technology" and thus had to be

---

[202] Interview with a Canadian telecommunications executive, January 31, 2012.
[203] Interview with a Canadian consumers advocate, January 30, 2012.
[204] Interview with a Canadian telecommunications executive, January 31, 2012.
[205] Interview with a Canadian telecommunications executive, January 31, 2012.
[206] Interview with a Canadian technologies journalist, February 3, 2012.
[207] Interview with a Canadian consumer advocate, January 30, 2012.

addressed because it is fundamentally "a wiretapping technology." The outcomes of advocacy, from this same person's perspective, are less positive: "Civil society can whip people up on an issue-by-issue basis but in the long-term erosion is harder to fight and I think that's more true for privacy than in any other area, particularly right now."[208] So, privacy is seen as having been successfully 'framed' by advocates, though the framing was largely around future potential uses of the technology and not existing applications of it.

Content Control

Content control as it applies to DPI has been an issue on the Canadian agenda in a somewhat oblique way. Rather than calls for DPI to monitor or mediate data traffic or to act on suspected copyright infringing content, concerns and contestations have revolved around ISPs prioritizing some content over other content. Public advocacy groups have raised such data prioritization practices as an issue and have had ILECs routinely dismiss their concern as a real issue. Content producers also raised concerns. They argued that producers who were not tightly linked with ISPs' broadcasting arms could experience discriminatory treatment if they decided to principally transmit content using real-time applications over the Internet.

PIAC argued that targeting particular established protocols meant that some users who communicated one way would be discriminated relative to those who communicated using applications that were not 'managed' by DPI. The consumer groups maintained that DPI's very purpose is to discriminate between certain kinds of traffic and, by extension, the users responsible for generating the traffic. This position was supported by CIPPIC/CDM, who wrote that DPI subjected P2P users to "unjust discrimination and an undue disadvantage" relative to non-P2P users who were transmitting content, and that DPI subjected "content providers who distribute their product via P2P protocols" to "an undue disadvantage." Further, the technology undermined Canadian policy meant to encourage "innovation in the provision of telecommunication services."[209] Adding to the

---

[208] Interview with a Canadian civil advocate, January 30, 2012.

[209] CIPPIC/CDM, "In The Matter of an Application by The Canadian Association Of Internet Providers ("CAIP") (Applicant) Pursuant To Part VII Of The CRTC Telecommunications Rules of Procedure and Sections 7, 24, 25, 27, 32, 36, And 62 of the Telecommunications Act directed to Bell Canada (Respondent) Requesting Certain Orders Directing Bell Canada to Cease and Desist From

chorus, corporate organizations such as Skype, the Canadian Association of Voice over IP Providers, and Google recognized that traffic management threatened to establish unfair discrimination against non-telco-controlled services.[210]

Parties worrying about content discrimination were not solely concerned about the potential privileging of ISP-driven Internet-based content. Parties such as the Campaign for Democratic Media,[211] PIAC,[212] the Canadian Film and Television Production Association, and the Independent Film and Television Alliance[213] noted that a problem *caused by* DPI was its capacity to support ILECs' existing broadcast-based revenue streams. Such support was made possible by deprioritizing, or slowing, P2P-transmitted content while ILECs' own online video portals and traditional broadcast services (e.g. IP television) were *not* affected by DPI. Here, DPI was a 'solution' meant to respond to the 'problems' that ILECs face, which were brought about by over-the-top services (e.g. VoIP) and content (e.g. YouTube and Netflix).

ILECs denied that packet deprioritization or bandwidth 'caps' on P2P applications would negatively affect non-targeted application types. Specifically, Shaw tried to avoid criticism by contesting the nature of their throttling behaviors. Because the company only shaped upstream P2P traffic and did not limit individuals from downloading content, it argued that it was not regulating behavior by driving customers to non-P2P content

---

"Throttling" Its Wholesale ADSL Access Services Comments of the Campaign for Democratic Media ("CDM")," *CRTC*, July 3, 2008, accessed April 22, 2012, http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923867.zip, Pp. 2-3.

[210] Google, "Comments concerning CAIP Part VII Application requesting certain orders directing Bell Canada to cease and desist from "throttling" its wholesale ADSL Access Services," *CRTC,* July 3, 2008, accessed March 3, 2012, http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923481.pdf.

[211] Campaign for Democratic Media, "Oral Submissions of Campaign for Democratic Media – Telecom Public Notice CRTC 2008-19: Review of the Internet Traffic Management Practices of Internet Service Providers," *CRTC*, July 9, 2009, accessed March 3, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241703.PDF.

[212] PIAC, "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers – Comments of the Consumers' Association of Canada, the National Anti-Poverty Organization and Option consommateurs ("The Consumer Groups")," *CRTC*, February 23, 2009, March 4, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030499.zip.

[213] The Canadian Film and Television Production Association and the Independent Film and Television Alliance, "Oral Remarks by The Canadian Film and Television Production Association and the Independent Film and Television Alliance - Telecom Public Notice CRTC 2008-19 – Review of Internet traffic management practices of Internet service providers," *CRTC*, July 8, 2009, accessed March 4, 2012, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241693.PDF.

sources (such as Shaw's traditional broadcast services).[214] Rogers[215] and Bell Canada[216] made similar assertions. These assertions did not address how slowing uploads affect download speeds; many P2P applications let users download files faster if they upload data quickly as well. Consequently, limiting upload speeds can hinder download speeds too. Further, parties questioned the targeted nature of DPI mediation, given Bell's and Rogers' inadvertent disruption of non-P2P protocols. Rogers, in particular, negatively affected video games' Internet traffic to the point where the Canadian Gamers Organization brought a complaint against the company.

In general, ILECs' arguments focused on *access* to others' communications and content versus the *distribution* of one's communications and the effect that slowing distribution had on the accessibility of cultural products. However, ILECs' efforts were often underscored by a normative logic that identified 'good' and 'bad' uses of Internet services. Cogeco implicitly saw DPI as part of a long-term 'training' of customer behavior. The company argued that billing customers based on actual bandwidth consumption – an economic traffic management practice – was far less effective than DPI because economic ITMPs cannot quickly adjust how customers use broadband access.[217] DPI, in contrast, enabled a rapid modification of habit and (Cogeco argued) habits must be changed so that all users can enjoy their broadband access *and* let the company mitigate congestion. Shaw argued that its uses of DPI were related to efficiency: the company was uninterested in censoring or watching the contents of data packets because the company is not an agent of the state; DPI was not a technical means to massively

---

[214] Shaw, "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers – Reply Comments," *CRTC*, April 30, 2009, accessed June 28, 2009, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/110988 5.pdf.

[215] Rogers, "Telecom Public Notice CRTC 2008-19 – Review of Internet traffic management practices of Internet service provider – Rogers Reply Comments," *CRTC*, April 30, 2009, accessed June 28, 2009, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/111039 2.pdf.

[216] Bell Aliant/Bell Canada (Bell), "Telecom Public Notice CRTC 2008□19, Review of Internet management practices of Internet providers (PN 2008- 19) – Comments," *CRTC*, February 23, 2009, accessed June 28, 2009, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/102980 4.zip.

[217] Cogeco, "CRTC File No: 8646-C12-200815400 - Telecom Public Notice CRTC 2008□19, Review of the Internet traffic management practices of Internet service providers □ Cogeco Reply Comments," *CRTC*, April 30, 2009, accessed June 28, 2009, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/111048 8.pdf.

inspect content in real-time flowing over their network; and any act of massive content-based surveillance would contravene the *Telecommunications Act*.[218]

While ISPs lost some degree of network control when the CRTC produced a decision concerning ISPs' prioritization of data traffic, it is debatable how significant that loss has been. Specifically, while services cannot be discriminated against to the point that the service's character or content is transformed – for example, by preventing VoIP services from functioning or by delaying data transfers for real-time content to the point where content could not load – situations where ISPs *have* discriminated against such services have not been accompanied by significant punishments.[219] This said, civil society and consumer groups can take some credit for changes in how the Commission addresses transgressions of the ITMP policy; one interview subject noted that while "the CRTC sometimes is too willing to take ISP assurances from the high-level VPs at face value without going any further,"[220] the result of publicly 'outing' the number of ITMP complaints the CRTC received after the ITMP hearing, led to significant changes at the CRTC. One Canadian telecommunications executive noted that this outing "was effective within the industry for raising the profile of the issue, because up until that point there wasn't very much visibility into how many complaints there were."[221]

The most high-profile criticism of ISPs discriminating against legitimate traffic, following the conclusion of the CRTC's ITMP proceeding, came when the Canadian Gamers Organization filed a complaint (with the assistance of Open Media and CIPPIC) about how online video games were being negatively affected by DPI-based traffic management. [222] Specifically, Rogers' equipment had been misconfigured so that it misclassified computer game data traffic.[223] Prior to, and during, the complaint a series of

---

[218] Shaw, "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers – Reply Comments," *CRTC,* April 30, 2009, accessed June 28, 2009, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/110988 5.pdf.
[219] Michael Geist, "Canada's Net Neutrality Enforcement Failure," *Michael Geist,* July 8, 2011, accessed June 27, 2012, http://www.michaelgeist.ca/content/view/5918/159/.
[220] Interview with a Canadian consumer rights advocate, January 30, 2012.
[221] Interview with a Canadian telecommunications executive, January 31, 2012.
[222] Nate Anderson, "Oops: major Canadian ISP admits throttling *World of Warcraft*," *Ars Technica*, March 29, 2011, accessed June 20, 2012, http://arstechnica.com/tech-policy/news/2011/03/oops-major-canadian-isp-admits-throttling-world-of-warcraft.ars.
[223] Christopher Parsons, "Rogers, Network Failures, and Third-Party Oversight," *Technology, Thoughts, and Trinkets*, December 2, 2010, accessed June 20, 2012, http://www.christopher-parsons.com/blog/isps/rogers-network-failures-and-third-party-oversight/.

news sources published articles outlining the issues with Rogers' throttling mechanisms.[224] Rogers was ultimately found to have violated the CRTC's decision concerning the legitimate use of technological traffic management tools.[225]

Some in the ISP community have been disquieted by how the CRTC reacted in response to advocacy groups' complaints, with one telecommunications executive stating, "I'm a bit surprised at the tone of the Commission's letter. From my understanding, they had a problem with online gaming and it was fixed – maybe it wasn't – but if it was fixed then I don't see what the issue is and what the enforcement is. If it wasn't fixed, well, that's one thing. I don't think the way they did it was necessarily the right way to do it. They should have just asked Rogers to submit … I think it was more of a public shaming than anything."[226] Thus, the open disclosure of Rogers' failures is seen an inappropriate and perhaps outside of the range of actions that the regulator ought to be engaged in.

Ultimately, copyright proper, while an issue for some members of the policy community, has not been a significant driver of how DPI has been used. Instead, emphasis has been on whether and how throttling could affect the distribution of legal content. While one telecommunications executive acknowledged that Canada's recent copyright legislation (C-11) and vertical integration of content owners and transmitters could encourage DPI being refocused for copyright purposes, no evidence of such a transition existed at the time of our interview. Another telecommunications executive worried that groups interested in blocking or censoring some material – including those associated with Hollywood – could develop an interest in using DPI to block content. Pushing back on these concerns, another telecom executive said, "I remember being approached by a copyright advocate saying, "Why did you never argue that peer-to-peer is only used for pirate copies?" It was never about that for us. I mean, it's really the

---

[224] Ernesto, "Rogers' BitTorrent Throttling Experiment Goes Horribly Wrong," *TorrentFreak*, December 13, 2010, accessed June 21, 2012, http://torrentfreak.com/rogers-bittorrent-throttling-experiment-goes-horribly-wrong-101213/. Karl Bode, "Rogers' New Throttling System Cripples Speeds And inadvertently impacting non-P2P applications," *DSL Reports*, December 14, 2010, accessed June 20, 2012, http://www.dslreports.com/shownews/Rogers-New-Throttling-System-Cripples-Speeds-111830.

[225] CRTC, "Re: File 545613, Internet Traffic Management Practices ("ITMP"), Section 36 of the Telecommunications Act, S.C. 1993, c. 38, as amended ("Act"), and Paragraphs 126 and 127 of Telecom Regulatory Policy CRTC 2009-657 ("TRP CRTC 2009-657")," *CRTC*, January 20, 2012, accessed June 20, 2012, http://www.crtc.gc.ca/eng/archive/2012/lt120120.htm.

[226] Interview with Canadian telecommunications executive, January 31, 2012.

impact on the network. And I think that the day we start getting into those types of arguments is a slippery slope towards being accused of controlling content." While specific accusations that P2P technologies were used for infringing purposes were typically avoided in regulatory proceedings, one executive stated "when it served the interests of the carriers that were defending [DPI] technology, they would never say explicitly that everyone knows peer-to-peer is used for piracy, but it was clearly part of the rhetoric."[227] Thus, while blocking specific content wasn't necessarily a live issue in Canada, implicitly limiting access to infringement-enabling technologies was useful when arguing against P2P technologies.

Since the initial CRTC decision some ISPs – such as Bell and Rogers – have agreed to stop using DPI to throttle data traffic. They have not, however, placed their own content distribution on an 'equal footing' with their over-the-top competitors; as a result, competitors may experience some delays in getting traffic to consumers over the public Internet, whereas ISPs' own content and service offerings can be delivered without delay over IPTV or VoIP by prioritizing their own services ahead of competitors. The policy network was largely supportive of decisions that prevented ISPs from inspecting content for copyright reasons, though implicit linking of P2P technologies with infringement was seen as a ground for supporting DPI-based throttling. Still, decisions from the OPC and CRTC alike meant that rights owners could not reasonably expect ISPs to start monitoring for infringement, which (arguably) satisfied some of the advocates' privacy concerns and ISPs' copyright liability worries.

If DPI was used for more invasive uses than it has been previously, such as identifying potential copyright infringement, then this type of practice would likely become a very live issue. One journalist said that while "the anticompetitive side is dying down, you know, a lot of the providers are cutting off the throttling … I think it's going to come raging back with privacy, especially if they start to look at things like cutting people off because of copyright issues."[228] Ultimately, then, while content management might be a 'quiet' issue now, it remains one that could quickly re-emerge as a heated issue.

---

[227] Interview with Canadian telecommunications executive, January 31, 2012.
[228] Interview with a Canadian technology journalist, February 3, 2012.

Advertising

Advertising was raised as a potential reason for how DPI had been, was being, deployed in Canada. Privacy-related concerns were put to both the Office of the Privacy Commissioner of Canada (OPC) and the CRTC. CIPPIC filed a complaint to the OPC against Bell, but the group encouraged the Commissioner to investigate a series of ISPs who were using the technology, including Rogers, Shaw, Cogeco, and Eastlink.[229] The core focus for CIPPIC was that personal information was being collected and that Bell had to adhere to the provisions of Canadian privacy law if they wanted to use DPI for traffic management purposes. Moreover, the advocacy group was mindful that the technology could "also be used to profile individual subscribers for marketing or other purposes."[230]

In supplemental evidence, CIPPIC focused explicitly on behavioral advertising. While this evidence drew from evidence of such advertising techniques in the United States and United Kingdom, it was also pointed out that Canadian press was reporting that the dominant American company, NebuAd, was looking to enter the Canadian market. Further, Bell Canada's supplier of DPI equipment had issued a press release that explained how tracking customers' Internet usage patterns could be used to optimize marketing.[231]

In reaction to CIPPIC's allegation, Bell disputed that it was collecting personal information. Relying on a non-OSI model of data packets – and thus disagreeing with the validity of the OSI model that was presented in Chapter Two – Bell insisted that it focused on the header of one layer of the data packet. This model separates payloads and headers at each level of the data packet. The consequences for this distinction are significant because the technical detail creates a difference in understanding what the appliance is or is not examining. Bell's explanation about how DPI functioned, what it did, and what it was capable of provided a key site of contestation because the explanation would have let Bell act on 'layer 7' OSI data without necessarily infringing

---

[229] CIPPIC, "Re: Bell Canada/Bell Sympatico Use of Deep Packet Inspection: PIPEDA Complaint," *CIPPIC*, May 9, 2008, accessed May 12, 2013, http://www.cippic.ca/sites/default/files/Bell-DPI-PIPEDAcomplaint_09May08.pdf.

[230] CIPPIC, "ISP Use Of Deep Packet Inspection (May/July 2008)," *CIPPIC*, updated September 2010, accessed May 12, 2012, http://www.cippic.ca/en/DPI.

[231] CIPPIC, "Supplement Letter to Complaint #6100-02744," *CIPPIC,* May 26, 2008, accessed May 12, 2013, http://www.cippic.ca/sites/default/files/Bell-PIPEDAsup1-behavioural%20targeting_26May08.pdf.

on communications privacy on the basis (the company claimed) that the content of packets would not be examined. Bell also asserted that it was not collecting personal information when using its traffic management systems. This same argument was presented by Bell – and countered by CIPPIC and the consumer groups – at the CRTC hearings concerning the use of DPI.

Ultimately, the OPC found that Bell was not collecting the information required to engage in DPI-driven behavioral advertising. The core of the decision revolved around the company having to be clearer on how, and why, it used DPI for traffic management purposes in its online documentation that was available to subscribers. However, Bell did acknowledge that if DPI were used "for a different purpose, e.g. marketing purposes, it would have to do so in compliance with the PIPEDA obligations, such that a new purpose would have to be identified, consent … would have to be obtained prior to doing so and the form of consent would depend on the sensitivity of the information. No consent would be sought on the actual technology being used to do so." The Commissioner, in the final paragraph of her decision, affirmed that should Bell use DPI to collect, manage, or disclose personal information "for purposes other than the current purpose of managing network traffic" then the company would, indeed, need additional and enhanced consent from individuals who were affected.[232]

Worries that DPI could be used for advertising purposes were also brought up at the CRTC. The Interactive Advertising Bureau of Canada raised concerns that Bell's actions could negatively affect selling online adspace,[233] and other parties were concerned that DPI could be used to track subscribers and insert ads into packet streams. External to the CRTC proceedings, at major Canadian telecommunications conferences in 2009, a host of vendors sought to sell ISPs on the idea of behavioral advertising, whereby ISPs could use DPI to track subscribers and subsequently deliver context-specific advertising to them. This was recognized and raised as an issue by some civil

---

[232] Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2009-010: Report of Findings Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection," *OPC*, September 2009, accessed May 12, 2013, http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.asp

[233] Interactive Advertising Bureau of Canada, "Comments Concerning - #: 8622-C51-200805153 - Canadian Association of Internet Providers (CAIP) - Application requesting certain orders directing Bell Canada to cease and desist from throttling its wholesale ADSL Access Services," *CRTC*, July 3, 2008, accessed March 20, 2012, http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923856.zip.

advocacy groups. In addition, these groups worried that DPI might be used for non-management activities. As summarized by the CRTC, these groups submitted that "personal information could be collected, stored, and potentially used for purposes other than traffic management without notification and consent. They considered this to be an invasion of privacy."[234] ISPs generally opposed any particular privacy enhancements based on the use of DPI, asserting that existing privacy regulations were sufficient and that DPI was not used to monitor the content of communications. Consumer advocates, in particular, were interested in getting the CRTC to establish terms around how, with one interviewee saying:

> We've tried to make sure [the Privacy Commissioner] has had no impact on CRTC proceedings because the problem is that the jurisdiction, such as it is, under 7(i) of the Telecom Act is so positive for consumers that anything else, like, even PIPEDA is garbage by comparison.[235]

On the basis that section 7(i) of the Telecommunications Act affirms that the CRTC is to "contribute to the protection of the privacy of persons,"[236] the Commission found that it could respond to privacy concerns stemming from uses of DPI. Further, given that PIPEDA operates as a 'floor' for privacy protection, the Commission saw that it could establish rules that were more privacy protective than those under PIPEDA. As such, it directed "all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information." Moreover, the Commission instructed the ILECs to modify their contracts with CLECs so that the personal information that

---

[234] CRTC, "Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers," *CRTC*, October 21, 2009, accessed June 6, 2013, http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm.
[235] Interview with Canadian consumer rights advocate, January 30, 2012.
[236] Government of Canada, "Telecommunications Act," S.C. 1993, c. 38, http://laws-lois.justice.gc.ca/eng/acts/T-3.4/page-2.html#h-6.

CLECs collected for traffic management purposes could not subsequently be used for non-management practices, nor could they disclose the collected information.[237]

To date, no Canadian ISP has used DPI for advertising, and the OPC and CRTC have established that any such usage has to be publicized before beginning. Given the stated non-interest in this kind of advertising, the issue has been regarded largely as a 'back-burner' item. Advocates 'won', but there was little indication that ISPs genuinely planned to conduct such activities in the first place.[238]

Policing and National Security

To date, DPI-based debates have focused on media control, traffic throttling, privacy, and marketing. The narratives surrounding the technology have largely avoided issues of copyright. In terms of using DPI for state surveillance and enforcement purposes, however, we may be witnessing a change to which agenda(s) the practices linked to the technology is situated on. Specifically, Canada's majority federal government, elected in 2011, has been strongly advocating for a series of lawful access powers.

Three types of powers – search and seizure provisions, communication interception, and subscriber data production – are typically associated with, and enhanced by, such legislation.[239] Policing bodies have aggressively advocated for the legislation[240] though they have faced considerable resistance to the proposed expanded powers. This resistance has led the Canadian Association of Chiefs of Police to canvass their members, writing "[i]t is imperative that we gather examples that can support the need for this legislation in the eyes of government, privacy groups, media, police and especially the public … The seriousness of this cannot be understated. We are therefore seeking your

---

[237] CRTC, "Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers," *CRTC*, October 21, 2009, accessed May 12, 2013, http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm.

[238] It should be noted that on October 22, 2013 – days before this dissertation was defended – Bell Canada announced they would launch a behavioural advertising system that monitored wireline and wireless subscribers' actions online. Bell's retail subscribers were given until November 16, 2013 to opt-out, and the Office of the Privacy Commissioner of Canada and civil society organizations had already begun to investigate the practice. So, while it is unclear if DPI specifically is being used for the advertising system it is evident that the issue of such advertising practices has prominently re-emerged on the Canadian agenda.

[239] CIPPIC, "What is "lawful access?"," updated June 2, 2007, accessed March 26, 2012, http://www.cippic.ca/en/lawful-access-faq#LA01.

[240] CBC News, "Online surveillance bill backed by police chiefs," *CBC News: British Columbia*, February 20, 2012, accessed June 22, 2012, http://www.cbc.ca/news/canada/british-columbia/story/2012/02/20/bc-police-bill-c-30.html.

support in gathering this information by instructing your members on the vital importance of providing the information to help bring these Bills into law."[241] DPI could facilitate these powers by improving the granularity of access to communications and could potentially be used to monitor the networks for the distribution of certain types of content or communications.

One telecommunications executive noted that government could, though it shouldn't need to, require ISPs to adopt DPI for lawful access solutions. This person also said that, "I guess for the technology, the companies that make the technology, they don't really care what the motivation is for using it, they just want to sell their products. So they'd be quite happy if governments said that all ISPs had to install technologies like theirs and use it for government-mandated reasons."[242] A Canadian consumer advocate raised concerns about the technology; the advocate could "only see DPI being used to dragnet stuff and data mine" in an effort to look "for what they think are criminal patterns."[243]

More generally, civil society advocates and the privacy community are mindful of the potentials of DPI for facilitating lawful access laws, but it remains unclear whether the policing community will enter the policy network that framed DPI. Both CIPPIC and Open Media (formally the Campaign for Democratic Media) have been actively involved in opposing the legislation, partnering with over forty organizations to oppose the legislation.[244] Public presentations that outline the potential dangers of the legislation have been given across Canada, often involving members of the Canadian academic privacy communities. Considerable media attention has been lavished upon the legislation and government agencies, and the federal Official Opposition has publicly come out against the broader surveillance capacities envisioned in the legislation. All of Canada's privacy commissioners have opposed how the legislation was drafted. In the

---

[241] Open Media, "Police Chiefs spend tax dollars to lobby for warrantless online surveillance," *OpenMedia,* January 18, 2012, accessed June 22, 2012, http://openmedia.ca/news/police-chiefs-spend-tax-dollars-lobby-warrantless-online-surveillance.
[242] Interview with Canadian telecommunications executive, January 31, 2012.
[243] Interview with Canadian consumer advocate, January 30, 2012.
[244] For a full list, see: http://openmedia.ca/SOS/members

face of significant public outcry, the government has withdrawn the legislation,[245] though the substance of the legislation may not be 'dead'. The issue of lawful access may, instead, have been shifted from the legislature to industry- and government-dominated policy domains addressing wireless spectrum auctions and regulation updates that dictate how telecommunications carriers must facilitate government surveillance of Canadians communications.[246]

ISPs are not seen as opposing lawful access itself, and they have not tended to oppose DPI either, which suggests that they may not rouse themselves to oppose DPI-mandated government surveillance so long as the surveillance is paid from public, rather than corporate, purses. Specifically, Bernard Lord, president of the Canadian Wireless Telecommunications Association, has stated: "We want to make sure the government is fully aware of all the costs and that they fully compensate all the costs … We feel it's really [parliamentarians'] job to decide what should be in the bill and companies will comply. But we want to make sure that parliamentarians and government realize that if they adopt this bill, these costs are attached to it."[247] In light of the new interception requirements that are being associated with current spectrum auctions, Lord stated to the Standing Committee on Industry that government should set aside some of the revenue from the auction to pay for any interception requirements.[248] This said, while one Canadian telecommunications executive asserted that they didn't think DPI was required for ISPs to meet prospective lawful access requirements, they conceded that now DPI "is more of a threat to the industry, something that may be imposed externally and the industry would be required to use it."[249]

---

[245] Steven Chase, "Ottawa hits pause on Web surveillance act," *The Globe and Mail,* February 24, 2012, accessed March 28, 2012, http://www.theglobeandmail.com/news/politics/ottawa-hits-pause-on-web-surveillance-act/article2349818/page1/.

[246] Christopher Parsons, "Lawful Access is Dead; Long Live Lawful Intercept!" *Technology, Thoughts, and Trinkets*, February 11, 2013, accessed April 9, 2013, http://www.christopher-parsons.com/lawful-access-is-dead-long-live-lawful-intercept/. Michael Geist, "Lawful Access is Dead (For Now): Government Kills Bill C-30," *MichaelGeist.ca*, February 12, 2013, accessed April 9, 2013, http://www.michaelgeist.ca/content/view/6782/125/.

[247] CBC News, "Online surveillance bill setup costs estimated at $80M," *CBC News: Politics*, February 22, 2012, accessed April 9, 2012, http://www.cbc.ca/news/politics/story/2012/02/22/pol-lawful-access-costs.html.

[248] Michael Geist, "CWTA Calls on Government to Use Spectrum Auction Proceeds to Pay for Lawful Access," *MichaelGeist.ca*, April 3, 2013, accessed April 9, 2013, http://www.michaelgeist.ca/content/view/6816/125/.

[249] Interview with a Canadian telecommunications executive, January 31, 2012.

Government, civil society advocates, and ISPs must all contend with the influence of vendors who have an interest in selling the equipment. Based on interviews, several telecommunications executives have suggested that some ISPs' decision to transition from DPI is the result of upgrading wireline networks.[250] Members of the advocacy communities hold similar positions.[251] Consequently, vendors' capacity to profit from 'pure play' network management DPI appliances may be on the decline if alternate uses cannot be found for the equipment. This situation may promote more aggressive vendor-advocacy for DPI as a solution to lawful access and interception problems. One telecommunications executive underscored that it is the sale of equipment – with reasons being secondary – that constitutes a 'win' for vendors. [252]

To date, lawful access legislation has not been passed by Parliament, but as the powers associated with it move to other spaces (i.e. spectrum auctions and regulatory updates) advocates' abilities to shape the media agenda to oppose how DPI might be used could be limited; these groups simply might not know what is being discussed or how DPI might be being used for state surveillance purposes. Further compounding framing efforts by these members of civil society may be the recognition by the CRTC, as well as by various parties who opposed DPI for throttling, that the equipment can legitimately be used for security purposes. When discussing DPI with regard to lawful access, one member of the privacy community stated that "[y]ou don't want to get paranoid with this stuff but you just don't know what kind of computing power people have, and I guess what I never really liked about DPI is … it's just like listening to conversations, really."[253] Another person interviewed, a journalist, doubted that the CRTC could do much of anything, if it decided to intervene, on the basis that "the CRTC is like a British police officer, where they run after somebody and yell, "Stop, or I'll yell stop again.""[254] So, if the policy domain significantly shifts beyond the CRTC, advocates may be significantly limited in how they can oppose lawful access practices involving DPI. Ultimately, it remains unclear whether the spectrum auction or regulatory updates will lead to DPI being used for lawful access, but, regardless, it is likely that the parties

[250] Interviews with Canadian telecommunications executives, January 31, 2012.
[251] Interviews with Canadian advocates, January 30, 2012.
[252] Interview with a Canadian telecommunications executive, January 31, 2012.
[253] Interview with a Canadian consumers rights advocate, January 30, 2012.
[254] Interview with a Canadian journalist, February 3, 2012.

involved in previous agenda-setting processes will need new approaches to shape DPI-based practices if security issues move to less accessible government domains.

Conclusion

DPI has been contested as either resolving, or establishing, problems as ISPs strive to enhance their control over their networks. ISPs have generally sought the ability to use the technology to mediate their own subscribers' traffic while contesting the right of ILECs to unilaterally use DPI to interfere with CLECs' data traffic. Consumer and civil advocates have tended to oppose the throttling of data on grounds that it is anticompetitive, that it is privacy invasive, and that the technology misclassifies data packets. Rights holders and other business interests also worry that by prioritizing some traffic over other traffic those who use the Internet as a distribution medium face competitive disadvantages.

The activities of this policy network can be divided into four 'episodes: the first and second episodes saw actors take up network management, neutrality, content control, and privacy issues related to the technology. Here, the CRTC and OPC were the dominant forums where parties sought to frame the technology as a boon or bane to Internet practices in Canada. DPI was seen as a 'solution' to the 'problem' traffic congestion – and, in an ancillary way, as a solution to threats to ISPs' revenues from telephony and content distribution products – or as a 'solution' that failed to address the underlying problems related to congestion on data networks and as an outright problem for fostering next-generation content distribution and access mechanisms. It was also during this period that Parliament and public protests occurred. The third episode arguably came after the second CRTC proceeding, when the Canadian Gamers Association filed a successful complaint against Rogers Communications' use of the technology and was significant in testing the post-CRTC decision framework. The fourth, and most recent, episode concerning lawful access has not seen DPI-proper on the agenda but hovering in the background instead. This episode is based on ongoing efforts by the federal government to enhance its legitimate surveillance powers. Whether DPI itself will be used as a tool to facilitate the exercise of these powers remains unclear. The specifics

of security measures have largely been steeped in ambiguity or national security/non-disclosure provisions.

In the first two episodes, despite limited attention by federal politicians, it was principally independent and specialized government institutions that evaluated the practices linked to DPI. In the case of the CRTC, the organization sought to avoid a 'network neutrality' hearing and instead focused on more defined policy issues. In contrast, the OPC refused to investigate how *all* ISPs in Canada were using the technology and instead opted to investigate Bell and then conducted education and awareness-raising efforts. At the conclusion of their respective investigations into the technology, the CRTC established guidelines for using the technology that included remedies if companies were found violating the guidelines, whereas the OPC established findings of fact and offered recommendations. The varying positions assumed by these government institutions speaks to the difference between the CRTC's power as a regulator and the OPC's reliance on soft power given its status as an ombudsperson. The actual testing of the decisions by both groups has been limited. Despite known infringements of the CRTC's guidelines, limited punitive consequences have befallen violators, and the OPC has not publicly released any other investigative findings concerning practices linked to DPI. This having been said, the OPC has been harshly critical of lawful access legislation and, along with other Canadian privacy commissioners, has been a significant player in opposing the legislation. Consequently, the shift of the debate from the public to more closed government processes (e.g. Industry Canada consultations and internal government updates to interception requirements for ISPs) may limit the OPC's ability to critique proposed uses of the technology as much as it limits the role of civil society advocates.

Overall, consumer and civil society advocates have to date been most successful in framing issues when they have tried to stop practices that have not yet manifested. While they may regard their efforts to preclude using DPI for copyright or advertising purposes as advancing the cause of consumer privacy, these were antecedent to the CRTC's core focus on network management. These advocates ultimately could not prevent – or significantly modify – corporate practices that were already in place.

On the whole, the Canadian situation reveals that contests were between a small network of policy elites. Those who were well entrenched and who 'controlled' the networks were permitted to continue their behaviors, though future practices such as behavioral advertising could not be implemented without prior governmental approval. Other parties influenced some of the practices related to DPI, but these parties were unsuccessful in significantly affecting incumbent ISPs' practices other than those privacy interests related to marketing and advertising. The Canadian case reveals what happens when a tight, elite group meets in regulatory spaces that are meant to deal with the kinds of issues linked to DPI-based practices but is less instructive of how non-specialist forums can influence the domestic regulations concerning the technology. In turning to the United States and United Kingdom, we will see what happens when a broader set of government institutions act as the arenas where DPI issues emerge to the political agenda.

Chapter 5: The American Experience

Since the turn of the millennium, academics and civil advocates alike have worried that American telecommunications companies could interfere with data transmissions and discriminate against competitors' offerings. Such concerns were aggravated following the Federal Communications Commission's (FCC) decision to "regulate down" and remove many of the common carrier provisions that telecommunications companies had been obliged to obey. In the aftermath of this change, one cable internet provider's decision to actively prevent P2P communications and other Internet Service Providers' (ISPs) use of deep packet inspection (DPI) for advertising brought the technology "onto the scene." Also, in this period, ISPs were discovered working with the federal government to conduct mass-surveillance without warrant. Included in the surveillance toolset were DPI technologies. In aggregate, these issues along with limited copyright discussions have propelled deep packet inspection onto a series of public agendas.

I begin this chapter by identifying the key policy actors who have taken an interest in DPI and the general positions they have adopted. Next, I turn to the various issues surrounding DPI: network management, copyright, advertising, and national security. When examining each issue area, I take up the technical, economic, and political dimensions that are relevant to the particular debates concerning each issue. Each section provides a description of the relevant issue and the associated policy actors who have been more and less effective at framing the issues at hand. The chapter concludes by briefly summarizing the key characteristics of the US policy network.

Introducing the Players

A recurring cast of actors exists in the policy networks that are invested in DPI and a handful of actors who have taken an intermittent interest in practices linked to the technology. Specifically, ISPs and civil society advocates have routinely clashed over how the technology is used, often with elements of the American government serving as, or involving themselves in, policy resolution arenas. Equipment vendors have been involved in the dissemination of the technology proper, though they are rarely involved in the public debates, and copyright holders have been (minimally) invested in the DPI

debates considering the technology's prospective capability to mitigate copyright infringement.

Many American ISPs are, to some extent, using DPI-based technologies. These companies have expressed interest in expanding how the technology is used from current wireline 'traffic management' purposes toward revenue generating practices such as ad injection. High degrees of broadband ownership concentration in the US that, when combined with an absence of meaningful contemporary common carrier provisions or federally regulated wholesale access to incumbent broadband networks, has led these companies to typically support one another to preserve the existing oligarchic market. Comcast, AT&T, Embarq, Verizon, and T-Mobile have figured in the debates, with Comcast, Verizon, and AT&T often wielding their influence to dull regulatory efforts and drum up "astroturf", or artificially created grassroots, support for their policy interests.[255] On the basis of common interests in minimizing applicable regulation and using DPI to enhance profits or mitigate expenses, American ISPs form a relatively stable policy community.

The core counterpoints to ISPs have come from two bases. Advocacy organizations, such as the Electronic Frontier Foundation, Centre for Democracy and Technology (CDT), and Free Press, have interests in privacy, digital rights, civil liberties, and consumer rights and interested academics who have variously supported these organizations' efforts. While different advocacy organizations have taken the lead on specific issues, prominent members of the American academic institutions have provided empirical research or theoretical frames that advocates and government bodies alike have used to ascertain and understand how DPI is used, could be used, and the significance of such uses. In many of the issue areas, advocates have focused on the privacy-infringing practices linked to DPI as well as how its deployment could undermine Internet-based market competition by establishing discriminatory pricing schedules. On the whole, this policy community tends to form a relatively unified group when DPI is used to aggressively undermine citizens' privacy, but they do not always agree. Solutions concerning how to respond and who should lead specific civil advocacy efforts can vary.

---

[255] Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press, 2013).

Vendors have been involved in many of the debates concerning the technology. The vendors tend to advocate either for their deployed solutions or, in other situations, to remain mute or unwilling to engage in public forums concerning the ways in which their technology is deployed or used. In yet other situations, their marketed materials have been used to fuel debates on the technology and its associated practices. Though supportive of selling DPI to ISP and government customers, vendors form a community with a limited public profile.

Turning to government itself, a variety of institutions have overseen the technology and provided spaces for members of the policy network to publicly discuss the technology. Traffic management issues have led to FCC actions. The Federal Trade Commission (FTC) has also taken part in the debate, focusing on when companies have modified subscribers' data and potentially violated their contracts with subscribers. American courts have provided the arena for actors' contestations surrounding DPI. Even when one actor has 'won' in one policy arena, other actors have sought to reverse those victories in legal challenges (and appeals). Given that some uses of the technology were *driven* by government, such as DPI's integration with government surveillance efforts, and the political nature of the aforementioned government institutions, these actors and institutions must be understood as deeply integrated members of the policy network. They are most assuredly *not* neutral.

Throughout the DPI debate, the media has been attentive, with the *New York Times* raising the use of the technology to the national agenda after breaking the story concerning America's warrantless wiretapping program.[256] Other major news sources, including the *Washington Post*, *AP*, and the *Wall Street Journal* have covered the technology. The technology trade press has also paid close attention to how DPI is used in America, with *Ars Technica*, *DSL Reports*, *Slashdot*, *P2PNet*, and *TorrentFreak* featuring prominently.

While the policy network has common players – ISPs and civil advocates are routine actors, and well-known media outlets and academics have spoken and written about the technology and its uses – the institutional domains in which the debates have

---

[256] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, accessed March 19, 2013, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

played out have varied. And, as has been previously noted, these domains are not neutral; when the FCC, the FTC, or the White House are involved in how the technology is or is not to be used, these organizations bring their own agendas to the table. So, in the case of the FCC, a core group of actors (ISPs, FCC Commissioners) have competed for the distribution of regulatory power after they more or less sidelined the consumer advocates who played a catalyzing role in initiating the FCC hearings. The policy network has opened up, however, where the FTC, Congress, and the Senate have been involved. Many members of this broader network had interests that were only tangentially related to the DPI discussion, and thus the discussions and actions amongst the network were more dynamic. Finally, when the Executive branch has been involved, it has either sought to actively preserve its perceived powers or to (not-so-subtly) threaten actors to take actions that the White House preferred or risk the Executive branch's wrath.

In summary, a set of divergent policy communities has participated in the policy network that has addressed DPI-related practices. ISPs compose one group. They tend to want to use DPI, or they have seen it integrated into their networks for state surveillance purposes. Civil and consumer advocacy groups have played a prominent role because they have been the principal community that has opposed both corporate *and* governmental practices that are linked with the technology. However, not all advocates have been equally involved on all issues: a division of labor, based on expertise, has often taken place. Vendors have played important roles insofar as they have advocated for some uses of the technology, and their literatures provided insights into how operators might use DPI. Finally, government organizations have played important roles in both setting the policy arenas where issues have been fought and as interveners. Members of these institutions often want to advance or protect their own interests. Media have also covered DPI in the US, and many of the issues became issues as a result of intense media scrutiny.

The Issues

Some actors have advanced deep packet inspection as a "solution" to a host of technical, economic, and political challenges, and other actors have suggested that it generates problems of its own. In what follows, I discuss how DPI has arisen on the US agenda by

way of a set of issues: network management, copyright, advertising, and national security. When discussing each of the issues, I remain attentive to the technical, economic, and technical affordances associated with the technology and its attendant practices. Issues in the United States often revolve around who is permitted to control, or monitor, subscribers' and citizens' communications, and the degree to which interference into those communications is appropriate and legal.

Network Management

Network management issues in the US have a long history. Before writing about how DPI is implicated in them, I outline the *Telecommunications Act* and its relevant Titles to put recent debates in context. Following this contextual information, I discuss how DPI is used to manage traffic. I focus on Comcast as the most important ISP in this debate, given the contest(s) it has had with its federal regulator, the FCC. Though civil society advocates were successful in initiating the FCC investigation of Comcast's practices, they were ultimately unable to intercede effectively after the matter left FCC jurisdiction. Ultimately, because of Comcast's debates and actions, ISPs have successfully advanced their interests, to the point where the FCC's ability to even regulate traffic management issues has been thrown into question.

Network management has been a prominent issue in the United States since the inception of the 1996 *Telecommunications Act*. The *Telecommunications Act* is divided into a series of Titles, which prescribe regulatory obligations for different end-type services. After the *Act*'s inception, Title II was applied to services that relied on copper wire and provided voice services, and companies that fell under Title II obligations were regulated as common carriers. In contrast, Title VI applied to broadcasters that used coaxial fiber cables to provide service. So, whereas traditional telecommunications companies (e.g. AT&T) fell under Title II, cable companies (e.g. Comcast) fell under Title VI and lacked common carrier obligations. Broadcasters that used airwaves fell under a third Title, Title III.[257] Under the *Act*, telecommunications companies (i.e. those that offered telephone-based Internet access) "had to give smaller companies access to

[257] Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press, 2013), Pp. 53-54; Jonathan E. Nuechterlein and Philip J. Weiser, *Digital Crossroads: American Telecommunications Policy in the Internet Age* (Cambridge, Mass.: The MIT Press, 2005).

their circuits, and the cable companies had to allow the Bells to compete with them for cable service."[258] These two information delivery-mediums, telephone lines and cable cables, were seen as establishing the conditions to mitigate monopolistic or oligopolistic powers over the flow of information across the public Internet. These intentions have not been born out in reality.

During his tenure as the Chairman of the FCC, Michael Powell sought to remedy what he saw as a problem: broadband Internet was regulated by three different Titles, depending on the type of network used for the communication. As a free market advocate, Powel sought to "regulate up" by "starting with a blank, unregulated slate" instead of "regulating down" by imposing Title II requirements on all broadband providers and subsequently 'tweaking' Title II obligations. Ultimately, the FCC declared that cable-modem service was an information service; this declaration relieved companies of Title II common carrier and interconnection requirements. After a Supreme Court challenge vindicated the FCC's decision concerning cable services, ADSL-based services were similarly classified as information services. As a result, wireline broadband Internet services were *all* relieved from common carrier requirements.

The FCC sought to placate critics who were concerned that the absence of common carrier requirements could lead to discriminatory practices with a 2005 *Internet Policy Statement*. That *Statement* outlined a series of freedoms for Internet users: access to content, access to applications, choice of devices, and competition among service providers.[259] At issue was the enforceability of the code. As will be evident from the discussion of DPI-based contestations associated with broadband services, those freedoms have not been enforceable with regard to how ISPs throttle their subscribers' data traffic.

Out-and-out blocking of applications on wireline broadband networks arose prominently as an issue in 2005 when a rural telephone company, Madison River Communications, blocked competing VoIP applications. This action led to an FCC investigation, out of which "Madison River and the FCC entered into a consent decree.

---

[258] Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press, 2013), Pp. 49.
[259] FCC, *FCC 05-151 Internet Policy Statement*, adopted August 5, 2005, accessed May 17, 2013, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

Madison River agreed to pay $15,000 to the US Treasury and to stop blocking VoIP applications; the FCC terminated the investigation."[260] While the dispute was resolved, it remains a central data point for consumer and civil advocates and academics who remain wary of telecommunications companies' desire to limit subscriber access to products that compete with the ISPs' own. The Madison River decision also failed to clarify the FCC's legal or regulatory power to stop such behavior. The concerns linked to ISPs blocking access to content or prohibiting certain data communications systems on wireline networks arose again in 2007 with Comcast's aggressive 'network management' practices, with the issue principally being taken up by the ISP, the FCC, and ultimately the courts.

In 2007, Comcast began actively interfering with peer-to-peer data connections. Comcast's subscribers noticed that P2P clients were not connecting to one another but the company publicly insisted that it was "not blocking any access to any application, and we don't throttle any traffic."[261] It was only after Robb Topolski, a computer networking expert, reported that Comcast was interfering with data traffic that Comcast altered how they explained the situation.[262] The company admitted that when P2P data traffic established a certain degree of congestion an RST packet was issued to terminate the P2P connection. The company maintained that such behavior occurred only "during periods of peak network congestion"[263] and only when such congestion was actually occurring on the network.[264] These statements were rebuffed by tests conducted by members of the public and were subsequently confirmed by the Associated Press (AP) and Electronic Frontier Foundation. In response, Comcast again modified its position and asserted that its P2P management system was triggered regardless of time of day or degree of network

---

[260] Barbara van Schewick, *Internet Architecture and Innovation* (Cambridge, Mass: The MIT Press, 2010), Pp. 241.
[261] Marguerite Reardon, "Comcast denies monkeying with BitTorrent traffic," *CNet*, August 21, 2007, accessed May 15, 2013, http://news.cnet.com/8301-10784_3-9763901-7.html.
[262] Robb Topolski ("Funchords"), "Comcast is using Sandvine to manage P2P Connections," *DSL Reports Forum*, May 12, 2007, last accessed September 7, 2013, http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections.
[263] Defendants' Memorandum of Law in Support of Motion for Judgment on the Pleadings at 6, Hart v. Comcast of Alameda, No. C-07-06350-PJH (N.D. Cal. Mar. 14, 2008) (Comcast Motion for Judgment)
[264] Letter from Mary McManus, Senior Director of FCC and Regulatory Policy, Comcast Corporation, to Kris A. Monteith, Chief, Enforcement Bureau, File No. EB-08-IH-1518, at 5 (Jan. 25, 2008) (Comcast Response Letter).

congestion.[265] Throughout FCC and court processes, Comcast insisted that its "network management practices were reasonable, wholly consistent with industry practices and that we did not block access to Web sites or online applications, including peer-to-peer services. We do not believe the record supports any other conclusion."[266] The company also cast users affected by the P2P interdiction as 'bandwidth hogs'; such 'bad' users were cast as inappropriately using network bandwidth and DPI-based throttling brought 'fairness' to the network.[267] Though Comcast has not been alone in throttling[268] or claiming the right to throttle P2P traffic,[269] the company has been the most aggressive in proactively delaying or preventing the use of P2P application protocols.

In the face of Comcast's early claims about how its P2P management system was targeted, Robb Topolski investigated the specific actions that the company was taking with regard to subscriber data traffic. He learned that the blocking of P2P connections occurred at the point where Comcast's networks connected with other points on the Internet and that Comcast was using RST packets, inserted by DPI appliances, to terminate P2P data connections that Comcast subscribers established. By inserting such packets, Comcast was deliberately interfering with its subscribers' communications. Topolski worked with the Associated Press to detail the technical characteristics of Comcast's actions;[270] the publicization of his research ultimately led the Electronic Frontier Foundation (EFF) to conduct its own investigations concerning Comcast's

---

[265] Letter from Kathryn A. Zachem, Vice President of Regulatory Affairs, Comcast Corporation, to Marlene H. Dortch, Secretary, FCC, at 5 (July 10, 2008) (Comcast Technical Ex Parte).
[266] Comcast, quoted in Nate Anderson, "Hammer drops at last: FCC opposes Comcast P2P throttling," *Ars Technica*, July 25, 2008, accessed January 30, 2012, http://arstechnica.com/uncategorized/2008/07/hammer-drops-at-last-fcc-opposes-comcast-p2p-throttling/.
[267] Dan Mitchell, "Say Goodnight, Bandwidth Hog," *The New York Times*, April 14, 2007, accessed May 16, 2013, http://www.nytimes.com/2007/04/14/technology/14online.html; Chloe Albanesius, "Comcast Cuts Off Bandwidth Hogs," *PC Magazine*, April 4, 2007, accessed May 17, 2013, http://www.pcmag.com/article2/0,2817,2111373,00.asp.
[268] Joe Mullin, "How ISPs will do 'six strikes': Throttled speeds, blocked sites," *Ars Technica*, November 16, 2012, accessed May 15, 2013, http://arstechnica.com/tech-policy/2012/11/how-isps-will-do-six-strikes-throttled-speeds-blocked-sites/.
[269] Timothy B. Lee, "Verizon called hypocritical for equating net neutrality to censorship," November 16, 2012, accessed May 15, 2013, http://arstechnica.com/tech-policy/2012/11/verizon-called-hypocritical-for-equating-net-neutrality-to-censorship/.
[270] Peter Svensson, "Comcast blocks some Internet traffic," *Associated Press*, published October 19, 2007, accessed May 17, 2013, http://www.nbcnews.com/id/21376597/.

actions that confirmed the AP's findings.[271] Together, the AP's and EFF's research identified that peer-to-peer connections were being disrupted, and they also learned that Lotus Notes and Windows Remote Desktop functionality was similarly disrupted, though subsequent adjustments to Comcast's injection protocols alleviated the unintended disruptions.[272]

In light of Topolski's findings and media attention, the Free Press filed a complaint to the FCC about Comcast's activities. Free Press asked the FCC to declare "that an Internet service provider violates the [Commission's] Internet Policy Statement when it intentionally degrades a targeted Internet application." A petition with the signatures of over twenty thousand Americans made a similar request, and a BitTorrent client company, Vuze, petitioned the FCC to adopt rules preventing ISPs from implementing policies or practices that discriminated against specific applications or content.[273]

While Comcast's actions *did* elicit a response from the civil liberties and consumer advocacy community, members that were predominantly interested in privacy were only minimally involved. As noted by Paul Ohm, Comcast's actions were largely situated in the domain of 'network neutrality' politics, and, at the time, there were activists who:

> watched quietly . . . The Electronic Frontier Foundation (EFF), for example, has mostly sat out the debate (although their technical work on the Comcast throttling was foundational.) EFF might not be able to resist getting more involved if the focus shifts to privacy, one of their two key issues (the other being Copyright law) and they should have much to say about the question of ISP monitoring. Another noticeably quiet voice has been the Electronic Privacy Information Center (EPIC). On the other side, the copyrighted content industries will see privacy-justified

---

[271] Peter Eckersly, Fred von Lohmann, and Seth Schoen, "Packet Forgery By ISPs: A Report on the Comcast Affair," *EFF*, November 28, 2007, accessed January 30, 2013, https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

[272] Peter Eckersly, Fred von Lohmann, and Seth Schoen, "Packet Forgery By ISPs: A Report on the Comcast Affair," *EFF*, November 28, 2007, accessed January 30, 2013, https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

[273] Free Press and Public Knowledge v. Comcast, 2008, FCC 08-183.

> restrictions on ISP monitoring as threats against tools they could use to protect their intellectual property.[274]

These same organizations, and specific actors who were responsible for the 'DPI file', would later focus on the invasive character of DPI and rally around its privacy-infringing characteristics. Their engagement in terms of network management, however, was muted. As a result, a fairly specialized subset of the public policy groups that were focused on network neutrality issues led the fight against Comcast's behaviors. In addition to identifying how DPI could threaten new business models, these groups framed the company's actions as clearly infringing on the FCC's Policy Statement.

As a result of media attention and the Free Press' filings, then FCC Chairman, Kevin Martin (who followed Powell), held two public hearings in 2008 at Harvard and Stanford. The first hearing saw Comcast pay people to take up seats and left dozens of 'real' participants outside and unable to contribute.[275] At the second, American telecommunications firms largely declined to attend and instead sent "proxies in their place: a conservative think tank called the Phoenix Center, freelance tech pundit George Ou, and one ISP: Lariat.net of Wyoming."[276] Moreover, the Commission received over 6,500 comments after the FCC's Wireline Competition Bureau requested comments on Free Press' and Vuze's filings.[277] At the conclusion of the FCC's process, it decided to neither impose an injunction or fine; instead the FCC "insisted that Comcast promise to adopt a protocol-agnostic method of network management by the end of 2008."[278] Moreover, the company had to:

---

[274] Paul Ohm, "The Rise and Fall of Invasive ISP Surveillance," University of Illinois Law Review 2009(5) (2009), Pp. 1495.
[275] Ben Fernandez, "Comcast Admits Paying Attendees at FCC Hearing," *The Philadelphia Enquirer*, February 28, 2008, accessed May 15, 2013, https://www.commondreams.org/archive/2008/02/28/7355.
[276] Peter Eckersley, "FCC Hearings at Stanford: Towards a Consensus on ISP Transparency?," *EFF*, published April 18, 2008, accessed May 13, 2013, https://www.eff.org/deeplinks/2008/04/fcc-hearings-stanford-consensus-isp-transparency.
[277] Federal Communications Commission, "FCC 08-183: Memorandum Opinion and Order," *FCC,* August 20, 2008, accessed August 23, 2013, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf.
[278] Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press, 2013), Pp. 58.

1. Reveal the "precise contours" of its network management practices, including the types of equipment used, when they came into use, how they were configured, and where they have been deployed.
2. Come up with a compliance plan complete with benchmarks that explain how Comcast will move "from discriminatory to nondiscriminatory network management practices by the end of the year."
3. Publicly disclose the details of its new practices, "including the thresholds that will trigger any limits on customers' access to bandwidth."[279]

The Commission's position both fit within the contours of its *Policy Statement* and sought to placate network neutrality advocates without forbidding the use of DPI or throttling of data traffic. The Statement provided hope to civil advocates that Comcast could successfully be identified as a villain that was responsible for breaking the tenets of the Statement and thereby victimizing business and 'regular' American broadband subscribers. It also suggested to these groups that the FCC might engage in enhanced oversight of Comcast's behaviours.

Rather than accept the Commission's decisions, Comcast appealed to the District of Columbia Court of Appeals. The appeal was based on Comcast's insistence that the FCC lacked regulations or authority to act on Comcast's usage of RST packets. The company's brief contended that "For the FCC to conclude that an entity has acted in violation of federal law and to take enforcement action for such a violation, there must have been 'law' to violate…Specifically, neither the *Policy Statement* that the FCC actually enforced against Comcast, nor the statutory provisions that the agency professed to enforce, are binding legal norms that governed the conduct at issue…**the *Policy Statement* is unenforceable as a matter of law**."[280] The FCC, in contrast, asserted that the Commission's 'ancillary jurisdiction', its ability "to regulate anything that affected

---

[279] Mathew Laser, "FCC Order scolds Comcast for changing story on P2P blocking," *Ars Technica*, August 20, 2008, accessed January 30, 2013, http://arstechnica.com/uncategorized/2008/08/fcc-order-scolds-comcast-for-changing-story-on-p2p-blocking/.

[280] Comcast, quoted from Scott M. Fulton, III, "Comcast may get legal leverage to stop net neutrality enforcement," *Betanews*, January 9, 2010, accessed May 2, 2013, http://betanews.com/2010/01/09/comcast-may-get-legal-leverage-to-stop-net-neutrality-enforcement/. Emphasis added.

the explicit subjects of its regulatory authority",[281] applied within the context of the *Statement*. However, because the FCC had previously classified wireline broadband service as an informational instead of telecommunications service, the common carriage provisions that might have applied prior to Powell's tenure as Commission Chair did not apply. So, the *Policy Statement* was seen as insufficient to regulate against problematic – that is, anti-common-carrier – uses of DPI appliances. As a result, in April 2010, Comcast won the appeal and the practical successes of consumer advocates in framing Comcast's actions to the FCC were undone.

Comcast *did* adopt an agnostic-throttling process, even though the company opposed the FCC's Order. Where the RST packet method injected packets into subscribers' data flows – using DPI to tamper with packet flows, contrary to how the applications were trying to communicate– the agnostic method did not require this degree of total packet awareness. Under the revised approach, customers experienced data throttling when network routers saw that the subscriber was involved in high-bandwidth activities for 15 minutes or longer; this approach saw a change in how packets were carried, insofar as the status of the subscribers' packets was reclassified to "best effort" from the default "priority best effort."[282] The agnostic method led to *all* applications being equally affected by Comcast's throttling solution and this method, so the company asserted, was needed because traffic was growing on its network at an unprecedented rate.

ISPs vis-à-vis Comcast have been highly successful in advancing the network management issue in their favor, having defended their classification as information services, rather than telecommunications services, and undermined the value of the FCC's policy principles and ancillary powers. In their strategy, they excised 'privacy issues' and, instead, emphasized their own legal right to unilaterally decide how to route traffic. Comcast was principally concerned with asserting its independence from the regulator, and to this end, Comcast escaped the FCC's domain and thwarted the regulator's attempts to maintain its own (limited) power. Subsequently, Comcast

---

[281] Jonathan E. Nuechterlein and Philip J. Weiser, *Digital Crossroads: American Telecommunications Policy in the Internet Age* (Cambridge, Mass.: The MIT Press, 2005), Pp. 24.
[282] Nate Anderson and Eric Bangeman, "Comcast loses P2P religion, goes agnostic on throttling," *Ars Technica*, September 19, 2008, accessed January 30, 2013, http://arstechnica.com/uncategorized/2008/09/comcast-loses-p2p-religion-goes-agnostic-on-throttling/.

successfully asserted its position to the courts. The courts focused exclusively on the legal contours of network management issues and ignored the public policy side of the issue.

Comcast's success left the FCC scrambling to regulate the industry it is tasked with regulating. The current state of affairs between the FCC and ISPs means that the telephony and cable-based ISPs in the United States have largely unregulated wireline Internet services with regard to network management; and the FCC may need legislation to be passed before the Commission regains its ability to regulate this issue. As a result, the most significant loser in the policy network has been the FCC itself; it has not just lost the setting of the agenda, but its very ability to regulate. While advocates were successful in setting the issue before the FCC, they were not similarly successful framing the issue before the courts. Still, despite the loss, Comcast did adopt the FCC-suggested means to throttle traffic. Ultimately, while the ISPs have almost certainly 'won' on network management, this victory is a combination of American deregulatory efforts, successful legal advocacy on the part of telecommunications companies, and (arguably) Comcast's shift from a predominantly policy-focused to legally oriented arena of contestation.

Copyright and Content Control

The potential to use DPI for mass content filtering purposes has raised significant concerns in the United States with civil society advocates and journalists alike warning that the technology's filtering potentialities could extend to blocking data transmissions that carry infringing files. Members of these communities have also warned that DPI could be used to control access to different Internet-based services and online destinations, such as Facebook. In what follows, I begin by briefly summarizing some relevant aspects of the American copyright debate to contextualize DPI's place in the broader discussion. Afterwards, I discuss the positions assumed by the relevant policy communities: ISPs, academics and civil advocates, copyrights holders, and the Executive branch of the US government. Ultimately, although DPI has been involved only minimally in the copyright debate, various parties have recognized it as a potential 'stick'

to encourage ISPs to adopt 'rights-friendly' policies without being required through legislation.

To fully appreciate the copyright debate in the United States as it relates to DPI, it is important to briefly explicate the history of recent American copyright reform. The United States has a history of expanding the powers available to copyright holders. Many of these powers limit access to, and dissemination of, copyrighted material. Section 512 of the Digital Millennium Copyright Act (DMCA) has been particularly significant in disputes between rights holders and service providers because it includes a provision that limits service providers' liability for transmitting, storing, or linking to infringing material. To take advantage of this provision, ISPs must establish policies to address subscribers who are found to infringe, the ISPs must have no knowledge of or gain financial benefit from the infringement, and ISPs must list an agent to deal with copyright complaints. So long as ISPs meet these requirements, they enjoy 'Safe Harbor'.[283]

Copyrights holders such as the Motion Picture Association of America (MPAA) and Recording Industry Association of American (RIAA) have lobbied aggressively for enhancing intermediaries' responsibilities.[284] Specifically, they have sought to require intermediaries (e.g. DropBox, Apple, Google, etc.) to pre-filter transmitted content and remove infringing material, or, if Internet companies do not comply, remove Safe Harbor protections. With this background in mind, I turn to discuss the positions taken by US actors with regard to copyright and controlling access to online content.

One manner of mediating access to content that might infringe upon copyright has revolved around blocking or throttling data protocols that copyright owners believe are linked to the infringing material. ISPs have rarely come out and insisted that using DPI to affect those protocols is directly related to copyright enforcement: instead, they have applied throttles, which tend to be linked to bandwidth management and conservation. In

---

[283] Chilling Effects Clearinghouse, "DMCA Safe Harbour," *Chilling Effects Clearinghouse*, accessed May 10, 2013, https://www.chillingeffects.org/dmca512/.

[284] Ken Fisher, "BSA doesn't think the DMCA goes far enough," *Ars Technica,* January 7, 2005, accessed May 1, 2013, http://arstechnica.com/uncategorized/2005/01/4511/; Mike Masnick, "RIAA Admits It Wants DMCA Overhaul; Blames Judges For 'Wrong' Interpretation," *Techdirt*, November 8, 2011, accessed May 15, 2013, https://www.techdirt.com/articles/20111108/00352916675/riaa-admits-it-wants-dmca-overhaul-blames-judges-wrong-interpretation.shtml; Mike Masnick, "PROTECT IP Renamed E-PARASITES Act; Would create The Great Firewall Of America," *Techdirt*, October 26, 2011, accessed May 15, 2013, https://www.techdirt.com/articles/20111026/12130616523/protect-ip-renamed-e-parasite-act-would-create-great-firewall-america.shtml.

the most extreme situation, as noted previously, Comcast was found to be injecting 'RST' packets into packet flows that were linked to the transmission of data that used P2P protocols. While Comcast's original actions did not block access to specific content, they did exert control over the means of *accessing* content. Amending data throttling so it became protocol agnostic arguably enhanced Comcast's interests, as one of America's dominant broadcasters, because Comcast's own services (e.g. IP-based TV offerings) did not activate the company's throttling systems whereas services from companies such as Netflix of Hulu would count towards activating the systems. With the agnostic approach, the company did not *block* access to content, but it does make its own content delivery systems more appealing to subscribers. Such 'agnostic' approaches effectively steer subscribers to ISPs' 'preferred' services. The same is true of other ISPs that throttle data traffic that is associated with services and content that compete with ISPs' own.[285] Importantly, such throttles "need not be blatant to be effective in steering customers to preferred content."[286] Adding a few extra seconds to buffer a video or download a song can nudge consumers towards an ISP's preferred distribution channels and, in the process, weaken the competitive positions of businesses offering competing products. Consequently, while the agnostic approach treats all competing data delivery systems – such as P2P applications, NetFlix, and YouTube – equally, it has the effect of affording preferential treatment to ISPs' own delivery mechanisms. A 'Madison River-type' of content blocking is not necessary for ISPs to discriminate against competitors' offerings.

American ISPs have generally resisted filtering or throttling for specific data *content* as opposed to throttling for specific data *application-types.* A recent technical analysis of P2P throttling in the United States shows a downturn in ISPs throttling applications that are commonly used to transmit copyright infringing files. Asghari, van Eeten, and Mueller hypothesized that this downturn ought not be the case because there ought to be a correlation between strong rights holder bodies and efforts to throttle data

---

[285] In the mobile environment, American telecommunications carriers routinely block access to services, such as video chat functions linked to Apple iDevices, or the ability to 'tether' mobile phones to other devices to provide Internet access. Access to such services is often predicated on paying a monthly fee.
[286] Shawn O'Donnell, "Broadband Architectures, ISP Business Plans, and Open Access," in *Communications Policy in Transition: The Internet and Beyond*, eds. Benjamin M. Compaine and Shane Greenstein (eds). (Cambridge, Mass.: The MIT Press, 2001), 53.

traffic. The authors interpreted the decrease in throttling to ISPs enjoying the "upper hand" in the debate with rights holders.[287]

The authors proposed reason for reduced throttling, however, does not necessarily account for the full politics of infringement; non-DPI-based mechanisms for mediating copyright infringement may simply be more politically feasible. Major US ISPs, despite the same companies' vigorous opposition to policies meant to restrict recidivist copyright infringers' access to the Internet, have recently voluntarily adopted a six-strikes policy instead of endorsing ISP-level filtering. ISPs did not think that their industry ought to be policing copyright infringement. AT&T wrote:

> Private entities are not created or meant to conduct the law enforcement and judicial balancing act that would be required; they are not charged with sitting in judgment of facts; and they are not empowered to punish alleged criminals without a court order or other government sanction. Indeed, the liability implications of ISPs acting as a quasi-law-enforcement/judicial branch could be enormous. The government and the courts, not ISPs, are responsible for intellectual property enforcement, and only they can secure and balance the various property, privacy, and due process rights that are at play and often in conflict in this realm.[288]

Other ISPs, such as Verizon and Comcast, offered similar comments at the time of consultation. The consequence has been that ISPs have not, to date, used DPI for overt copyright infringement surveillance; instead the ISPs' DPI systems have passively moved consumers to ISPs' own services or left rights holders to identify potential infringement. In aggregate, ISPs have sought to identify P2P users as problems on the basis that these users negatively affect Internet access for all subscribers. Simultaneously, ISPs have tried to characterize themselves as innocent of encouraging their subscribers' infringing

---

[287] Hadi Asghari, Mechel van Eeten, and Milton Mueller, "Unraveling the Economic and Political Drivers of Deep Packet Inspection: An empirical study of DPI use by broadband operators in 75 countries," *GigaNet 7th Annual Symposium,* November 5, 2012, Baku, Azerbaijan. Pp. 17.

[288] AT&T, "Re: Request for IPEC for Public Comments Regarding the Joint Strategic Plan (Fed. Reg. Vol. 75, No. 35 – FR Doc. 2010-3539)," *Whitehouse.gov*, March 24, 2010, accessed March 4, 2013, http://www.whitehouse.gov/sites/default/files/omb/IPEC/frn_comments/AT_T.pdf

behavior. Though successful with regard to the former, these companies' adoption of six-strikes policies bely their doubts that they would be cast as 'innocent' victims with regard to enabling access to copyright-infringing behavior.

Civil advocates and academics have long worried that ISPs might independently seek to 'address' the problem of copyright infringement. Many worries related to using technical architectures to act on individuals' online freedoms – such as sharing potentially infringing content – stem from Lawrence Lessig's influential book, *Code*. In it, Lessig argues that developers and engineers are dominantly responsible for establishing the 'laws' of the Internet and its associated services and products. *Code* addresses how freedom of expression can be negatively affected when digital code assumes the properties of law. Lessig asserts strong preferences for legislation, as opposed to Code, as a means through which to limit the sharing of copyrighted material, identifying the state as best suited to limit speech in a nuanced manner. Lessig specifically worries, however, that tasking private actors with the job of identifying and filtering speech would result in "more speech blocked than if the government acted wisely and efficiently."[289]

This line of argumentation is consistent with Goldsmith's and Wu's 2006 position. They assert that the American government will avoid overly stringent techniques to identify and block speech on the basis that filtering and blocking 'bad' speech "can only be stopped at the expense of giving up things that government and society value highly – like artistic expression and an open environment for speech."[290] It is this emphasis on the benefits of speech – and potential consequences of limiting speech – that has undergirded a significant amount of the intellectual discussion concerning network neutrality and associated concepts in the US DPI debates; if speech was analyzed or limited algorithmically, there would be economic,[291] privacy,[292] and

---

[289] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006), Pp. 255.
[290] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Toronto: Oxford University Press, 2006), Pp. 83.
[291] Barbara van Schewick, *Internet architecture and innovation* (Cambridge, Mass.: The MIT Press, 2010).
[292] Alissa Cooper, "The singular challenge of ISP use of deep packet inspection," *Deep packet inspection Canada*, published 2010, accessed January 3, 2013, http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deeppacket-inspection/.

constitutional implications.[293] Blocking content on the basis of prospective copyright infringement would raise all of these kinds of issues.

These concerns have been taken up by prominent US civil liberties groups. Organizations such as Free Press have focused on the network neutrality implications of DPI and identified how throttling or blocking applications or data content could have a negative effect on the availability of legal content and affect freedom of speech. Specifically, the organization has written about how ISPs could be motivated to charge for access to some content or some web sites, and it has pointed to vendors' publications as demonstrations that ISPs are being courted with systems capable of such interference.[294] Other organizations became involved when legislators sought to introduce language to Senate stimulus bills that would mandate ISPs to filtering data traffic for potentially infringing content; the Centre for Democracy & Technology, along with members of the Open Internet Coalition (which included major web companies, such as Skype and Google) successfully advocated against amendments that would authorize or require such filtering.[295] Organizations such as Free Knowledge and the New America Foundation's Open Technology Institute have also complained to regulators when ISPs, such as AT&T, blocked access to services or applications without subscribers first paying the AT&T a discrete fee to access those services.[296]

These civil and consumers rights groups' work has been supplemented by that of academics who have similarly warned that algorithmic filtering by ISPs could have a deleterious effect on freedom of expression. Scholars such as van Schewick have conducted economic analyses to make the financial interests that can motivate ISPs to control access to competing Internet services clear. When preventing or stymying access would result in higher revenues and not cause subscribers to switch ISPs, ISPs will be

---

[293] Angela Daly,"The legality of deep packet inspection," *First Interdisciplinary Workshop on Communications Policy and Regulation "Communications and Competition Law and Policy—Challenges of the New Decade,"* 2010, accessed January 5, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024.

[294] M. Chris Riley and Ben Scott, "Deep Packet Inspection: The End of the Internet As We Know It?" *Free Press*, March 2009, accessed March 1, 2013, http://www.freepress.net/sites/default/files/fp-legacy/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf.

[295] David Sohn, "Content Filtering Kept Out of Broadband Stimulus, At Least for Now," *Centre for Democracy & Technology*, February 11, 2009, accessed May 11, 2013, https://www.cdt.org/blogs/david-sohn/content-filtering-kept-out-broadband-stimulus-least-now.

[296] David Kravets, "Net Neutrality Groups Challenge AT&T FaceTime Blocking," *Wired*, September 18, 2012, accessed May 1, 2013, http://www.wired.com/threatlevel/2012/09/factime-fcc-flap/.

motivated to interfere in what subscribers can access. Given the limited competition between ISPs in most American markets, market competition cannot be seen as a way to 'solve' such bad behaviors. Moreover, the weakness of the FCC means that its ability to regulate good market behaviors is severely limited.[297] In aggregate, this policy community has sought to frame DPI as a problem insofar as it could affect the economic potentials of the Internet and prevent the realization of constitutional right. ISPs have been cast as villains. Though members of this community are often high-profile actors in issue-related policy arenas, their assertion that DPI is a problem has had limited uptake in the relevant arenas.

Although ISPs have not, to date, been forced to identify prospective copyright infringement, colleges and universities have been forced to adopt technology-based deterrents. Universities have sought to be careful in what they adopt because actively identifying or blocking content that crosses their networks could result in the loss of their Safe Harbor status. As such, administrators at universities like Syracuse University have adopted firewalls that block all P2P connections on campus; while this action does not directly address copyright infringement, it has reduced charges that its students and employees are infringing on rights holders' content.[298]

In terms of direct opposition to using DPI as a monitor for copyright infringement, there has been relatively little activity. Only universities tend to have adopted DPI or protocol-blocking firewalls to explicitly address infringement, often because some federal funding requires campuses to adopt technical systems to combat infringement.[299] While such requirements have raised alarms with educators and their related policy networks, members of the civil and consumer rights community more generally have not substantively campaigned against these requirements.

In contrast to ISPs and civil rights groups, some rights holders have asserted that the growth of broadband is tightly coupled with the availability of – and willingness to let subscribers access – vast online repositories of infringing content. The Songwriters Guild of America, as an example, has stated that:

---

[297] Barbara van Schewick, *Internet Architectures and Innovation* Cambridge, Mass.: The MIT Press, 2000).
[298] Milton Mueller, Andreas Kuhn, and Stephanie Michelle Santoso, "Policing the Network: Using DPI for Copyright Enforcement," *Surveillance and Society* 9(4) (2012): 348-364.
[299] Mueller, Milton; Kuehn, Andreas; and Santoso, Stephanie Michelle, "Policing the Network: Using DPI for Copyright Enforcement," *Surveillance and Society* 9(4) (2012): 348-364.

> Certainly (the ISPs) rolled out broadband based on movie and music downloads, legal and illegal and claimed (exemption from any legal responsibility), but at this point I think they realize being good partners with the content industry is a better idea. I really want to salute them for doing that.[300]

In 2009, Castro, Bennett, and Andes perhaps best summarized industry demands; in addition to changing social controls and amplifying legal capabilities available to rights holders to 'solve' the infringement problem, they also strongly argued that ISPs should deploy technical measures to counter infringement activities. They specifically asserted that DPI is an appropriate technical tool in the fight against infringement, for the following reasons:

1. Copyright filters are proven technologies, with YouTube as the example, and could be effective if ISPs were more broadly required to filter data traffic against 'fingerprints' of known infringing material.
2. DPI does not add latency and, even if it does, offline analysis – which would not have a noticeable impact on latency – could suffice to identify and prosecute infringers.
3. The fact that users engage in technological arms races is irrelevant; DPI is still a useful instrument for applying copyright policy.
4. While there are claims that DPI for infringement analysis could be costly, such claims should not prevent deploying DPI in production environments to ascertain the veracity of such claims.
5. Even if the technology cannot stop the transmission of infringing files, it could be used to prevent the usage of applications and protocols that are prominently used to transfer potentially infringing files. Thus, by targeting 'bad protocols' innovations in infringement might be delayed because the infrastructure has been made into a hostile communications space.

---

[300] Rick Carnes, quoted in Greg Sandoval, "Sources: AT&T, Comcast may help RIAA foil piracy," *CNet*, January 28, 2009, accessed March 8, 2013, http://news.cnet.com/8301-1023_3-10151389-93.html.

6. No freedom of speech concerns are raised because authors could – and should – pay rights holders to engage in speech if the DPI appliances would identified parody or satire speech as infringing.
7. If law precludes packet-level analysis for copyright – perhaps on grounds that this constitutes wiretapping – then the law should be modified to permit packet analysis for anti-infringement activities.[301]

Rights holders have worked through the White House 'Copyright Czar' who is tasked with intellectual property issues and Vice President Biden to advance their interests. As part of what is seen as an arm-twisting exercise, the Executive branch of the government aggressively lobbied major ISPs to adopt the six-strikes program – which would impose some kind of broadband access penalties to recidivist infringers of copyright – or face more onerous requirements that might follow from legislative actions.[302] Such legislative requirements might include DPI-based filtering capabilities.[303] Those lobbying efforts have been well received by the rights-holding community, and poorly by the ISP and civil liberties communities. Ultimately, DPI has not become the mechanism that is being used to monitor for infringing behavior; alternate mechanisms have been found instead. But DPI was a possible 'stick' that was advanced by lobby groups that met with members of the White House. Currently the adoption of a 'six-strikes' regime, where subscribers must be identified as infringing on copyright multiple times before the most serious consequences befall them, seems to have resolved the question of whether DPI should be used for enforcement actions. It should be noted, however, that this regime does not appear to be particularly accurate in terms of

[301] Daniel Castro, Richard Bennett, and Scott Andes, "Steal These Policies: Strategies for Reducing Digital Piracy," *The Information Technology & Innovation Foundation,* December 2009, accessed February 27, 2013, http://www.itif.org/files/2009-digital-piracy.pdf.
[302] Nate Anderson, "White House: we "win the future" by making ISPs into copyright cops," *Ars Technica,* July 7, 2011, accessed March 4, 2013, http://arstechnica.com/tech-policy/2011/07/white-house-we-win-the-future-by-making-isps-into-copyright-enforcers/; Timothy B. Lee, "ISP flip-flops: why do they now support "six strikes" plan?" *Ars Technica*, July 10, 2011, accessed March 4, 2013, http://arstechnica.com/tech-policy/2011/07/why-did-telcos-flip-flop-and-support-six-strikes-plan/.
[303] Personal correspondence with lobby group, July 2011.

identifying infringing works,[304] and it has already attracted some (limited) political opposition to the six-system.[305]

So, what does this mean in terms of actors and their arrangement? It means that while copyright infringement and, to an extent filtering for infringement, has been a high-priority agenda item, DPI has not been prominently linked to responses to the stated infringement problem. Controlled access to content has been, in comparison, a more significant issue. Although DPI has been contemplated as a mechanism to prevent some infringement – and, indeed, some data protocols are blocked at Universities to stymie infringing behavior – alternate mechanisms have been adopted. Advocates have raised concerns about the (in)appropriateness of blocking or throttling certain data protocols, often in relation to such throttling being an infringement of freedoms of expression, concerns that are similar to those stemming from network management. The previously discussed losses at the FCC level, have, however, prevented legal efforts from gaining traction and loud-spoken, advocates' messages have not moved beyond one of many agenda items. ISPs have generally disdained notions that they might be required to throttle for copyright purposes. And some rights holder lobby groups, while they have suggested using DPI for filtering, have found alternate paths to achieve their ends.

Ultimately, the use of DPI for copyright infringement has been a background threat to ISPs: they are to 'better cooperate' with meeting rights-holders' aims, or they risk facing legislation that will assist the enforcement of copyright. The interjection by the White House, combined with legislative bodies that have been receptive to copyright modifications that adhere to lobbying groups' interests, has led major ISPs to capitulate and accept a warning system. The general lobbying power of rights holders forced ISPs to avoid turning into villains that used network surveillance technologies against subscribers to combat copyright infringement. To date, neither the courts, the FTC, nor the FCC have been involved with regard to the 'six strikes' agreement. As a result, arenas

---

[304] Cyrus Farivar, "Here's what an actual "six strikes" copyright alert system looks like," *Ars Technica*, February 27, 2013, accessed March 4, 2013, http://arstechnica.com/tech-policy/2013/02/heres-what-an-actual-six-strikes-copyright-alert-looks-like/.

[305] Mike Masnick, "NJ Gubenatorial Candidate Speaks Out Against Six Strikes: ISP Shouldn't Decide What You Can Download," *TechDirt*, February 25, 2013, accessed March 4, 2013, https://www.techdirt.com/articles/20130225/10340922100/nj-gubenatorial-candidate-speaks-out-against-six-strikes-isp-shouldnt-decide-what-you-can-download.shtml.

where the ISPs might have had more sway have been kept out of the institutional arrangements.

The victors to date have been the copyright holders and the White House. Together, they framed the copyright infringement issue and exerted their influence without having to involve the legislature directly. This indirect measure of influence is significant, insofar as it means that the White House has not formally advanced a law or policy that would require ISPs to identify and help police certain speech/data transmissions: only private actors – the rights holders and ISPs – are involved. Thus, the White House may have realized its own goal (satisfying rights holders for political purposes) without potentially becoming embroiled in First or Fourth Amendment legal challenges. Although the current policy network is relatively inactive, it will likely become re-energized if the MPAA, RIAA, or other lobbying group, aggressively try to expand on their six-strikes compromise and impose active monitoring for infringing behavior on American ISPs.

Advertising

Advertising has become an increasingly significant part of the Internet-based economy. In 2008, some American ISPs began trials on a behavioral advertising system produced by NebuAd, a start-up that sold a product to track ISPs' subscribers and subsequently target subscribers with advertising. Potential revenue drove ISPs' interest in the technology and, ultimately, significant public backlash drove ISPs away from the technology. After briefly outlining how NebuAd's system worked, I discuss the policy communities who were involved, their positions in relation to one another, and analyze NebuAd's ejection from the US market.

As the core independent researcher of the NebAd system, Robert Topolski, conducted a report of NebuAd's actions. He found that the system monitored users' requests for non-encrypted (HTTP) webpages and "altered the inspected traffic; the IP header remained largely intact while the payload was changed by injecting Javascript…NebuAd used IP addresses, together with further information that could uniquely identify a users' computer, a hash code based on the ISP's customer record and

cookie preloading."[306] After tracking had begun, the NebuAd system created a profile about the individual and presented advertisements to subscribers that were based on their browsing habits.

The implications for NebuAd's systems were significant. Topolski argued that the company's actions bore resemblance to a browser hijack because the browser's normal behavior (i.e. just accessing the desired website) was being modified. Moreover, NebuAd's actions acted as a serious cross scripting attack because the browser was being led to believe (incorrectly) that the accessed website was making a formal request to NebuAd's advertising network. There were also similarities to Intel's 1999 controversy around embedding serial numbers within computer processors, a controversy that revolved around websites identifying returning visitors by reading their computer processors' serial numbers. Finally, the nature of modifying the content in transit bore resemblance to a man-in-the-middle attack, when a third party intercepts data from both the initiating and responding points and modifies the message before sending the data to its destination.[307] For all of these reasons, Topolski ultimately asserted that NebuAd's methodology of tracking ISP subscribers and delivering advertisements constituted an "attack" on subscribers' browsers.[308]

In late 2007 and early 2008, some American ISPs began trialing the NebuAd behavioral advertising system. CenturyTel and CableOne began in 2007. The 2007 deployments were met with relatively little fanfare, but the issue became more mainstream when, in March 2008, the ISP WideOpenWest (WOW) began "forcing connections and cookies" on its subscribers' computers, when, for example, the subscribers were browsing to Google.com. A popular telecommunications website, *DSL Reports*, reported on WOW's actions and the behavior corresponded with a minor change

---

[306] Andreas Kuhn and Milton Mueller, "Profiling the Profilers: Deep Packet Inspection for Behavioural Advertising in Europe and the United States," *SSRN*, September 1, 2012, accessed March 1, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181, Pp. 7.

[307] Robert M. Topolski, "NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking," *Free Press* and *Public Knowledge,* June 18, 2008, accessed February 5, 2013, http://www.freepress.net/sites/default/files/fp-legacy/NebuAd_Report.pdf. Pp. 9

[308] Robert M. Topolski, "NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking," *Free Press* and *Public Knowledge,* June 18, 2008, accessed February 5, 2013, http://www.freepress.net/sites/default/files/fp-legacy/NebuAd_Report.pdf.

to WOW subscribers' terms of service.[309] Similarly, in May, Charter Communications informed its customers that it would be "enhancing" subscribers' experiences by monitoring webpages that the subscriber visited and substituting their own ads for those that might otherwise be displayed. The company's communication was quickly disclosed to the forum[310] of *DSL Reports*. By the end of March, 2008, at least 416,000 subscribers had been enrolled in the NebuAd system, with subscribers belonging to WOW!, Embarq, CenturyTel, Knology, Broadstripe, Bresnan, and CableOne.[311]

Though media was initially skeptical of NebuAd's technologies, it wasn't outright hostile; the *New York Times' Bits* blog ran a story headlined "NebuAd Observes 'Useful, but Innocuous' Web Browsing."[312] NebuAd – and press that covered it – focused on ISPs being responsible for informing their users of NebuAd's presence and actions. The skepticism, and general trust in NebuAd's processes, changed dramatically as some members of the public learned that the DPI-based advertising system was being deployed. Two days after Charter proactively notified hundreds of thousands of subscribers about the system, Rep. Edward Markey, the Chairman of the House Subcommittee on Telecommunications and the Internet, and Rep. Joe Barton sent a letter to Charter questioning the nature of the advertising system. Their letter stated that

> Any service to which a subscriber does not affirmatively subscribe and that can result in the collection of information about the web-related habits and interests of a subscriber, or a subscriber's use of the operator's services, or the identification of an individual subscriber, and archives any of these results without the 'prior

---

[309] Robert M. Topolski, "NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking," *Free Press* and *Public Knowledge,* June 18, 2008, accessed February 5, 2013, http://www.freepress.net/sites/default/files/fp-legacy/NebuAd_Report.pdf.

[310] cjhort, "[HSI] Charter to monitor surfing, inserts its own targeted ads," *Broadband DSL Reports* (forum), May 10, 2008, accessed February 5, 2013, https://secure.dslreports.com/forum/r20461817-HSI-Charter-to-monitor-surfing-insert-its-own-targeted-ads.

[311] Andreas Kuhn and Milton Mueller, "Profiling the Profilers: Deep Packet Inspection for Behavioural Advertising in Europe and the United States," *SSRN*, September 1, 2012, accessed March 1, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181, Pp. 21.

[312] Saul Hansell, "NebuAd Observes 'Useful, but Innocuous' Web Browsing," *New York Times Bits* (blog). April 7, 2008, accessed February 5, 2013, http://bits.blogs.nytimes.com/2008/04/07/nebuad-observes-useful-but-innocuous-web-browsing/.

written or electronic consent of the subscriber,' raises substantial questions related to Section 631.[313]

Section 631 addresses the Communications Act, and the privacy provisions that apply to cable operators. In light of public criticisms, some ISPs put their adoption of NebuAd's product on hold. Charter, CenturyTel, and Embarq, for example, all delayed their plans to go forward with the technology, although not all ISPs did. Despite these delays, NebuAd did not stop looking for additional ISP partners.[314]

A series of lawsuits were also launched against the participating ISPs and NebuAd; many of the cases against the ISPs were dismissed because of jurisdictional boundary questions, and in situations where the cases went forward, the ISPs asserted that because it was NebuAd's technologies that conducted the data analysis, the ISPs themselves were exempt from prosecution. More directly, they asserted that the ECPA contemplates only "primary liability", which the ISPs asserted absolved them of wrongdoing because, again, the technology belonged to NebuAd. In their argument, the ISPs characterized themselves as mere supporting actors and, thus secondary, participants. Two of the smaller ISPs, Knology and WOW, asserted that they were also immune from secondary liability – or being liable for facilitating NebuAd's actions – on the basis that no general presumption of secondary liability exists in civil cases.[315] ISPs, generally, sought to first assert the NebuAd product as a positive thing for subscribers. When that position and the promise that the ad system protected privacy failed to resonate, ISPs dropped NebuAd to avoid being labeled as greedy or invasive of subscribers' privacy.

---

[313] Edward J. Markey and Joe Barton, "May 16, 2008 - Markey, Barton Raise Privacy Concerns About Charter Comm.," *House.gov*, May 15, 2008, accessed February 6, 2013, http://markey.house.gov/press-release/may-16-2008-markey-barton-raise-privacy-concerns-about-charter-comm.

[314] Center for Democracy & Technology, "An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd system and Other Uses of Internet Traffic Content from ISPs for Behavioural Advertising," *Center for Democracy and Technology,* July 8, 2008, accessed February 6, 2013, https://www.cdt.org/privacy/20080708ISPtraffic.pdf. Pp. 2.

[315] Nate Anderson, "ISPs: don't blame us; NebuAd did all the dirty work!" *Ars Technica*, February 6, 2009, accessed February 7, 2013, http://arstechnica.com/tech-policy/2009/02/isps-who-used-nebuad-hey-they-did-all-the-dirty-work/.

NebuAd established a privacy board through the Ponemon Institute in 2007, before launching their product, to defray privacy concerns. [316] In aggregate, the company sought to establish a 'privacy protective' means of monitoring ISP subscribers' actions online and sought advice from "highly respected privacy experts in the industry" to validate the company's approaches.[317] Beyond the Ponemon's involvement, who the specific experts were is unclear. As a vendor, the company was focused on selling its product and externalized responsibility for the manner in which the product was deployed to its customers, the ISPs.

NebuAd attempted to focus on the privacy-protective nature of its product. However, when NebuAd's CEO was called before a Senate committee and asked by Senator Byron Dorgan whether or not the company's product involved wiretapping, the company's CEO responded "My lawyers have told me we're in compliance with the law."[318] The company maintained that self-regulation was sufficient, that any privacy regulation should focus on sensitive information, and such regulations ought not to stifle innovation. Moreover, the advertising system was proposed as beneficial to consumers because it helped ISPs pay for infrastructure upgrades stemming from increased use of the Internet, which kept consumers' cost for Internet use down.

As a result of the hearings, the negative press, and the consequent retreat by the carriers, NebuAd was forced to modify its business model. The company's CEO resigned, and many of its staff were laid off in July and August of 2008.[319] Further, in September 2008, the company put its DPI-based tracking on hold, writing "With the Internet service provider channel currently on hold with the events of the summer, we

---

[316] NebuAd, "NebuAd Announces Privacy Council," *Business Wire*, November 5, 2007, accessed February 5, 2013, http://www.businesswire.com/news/home/20071105005667/en/NebuAd-Announces-Privacy-Council.

[317] Ashiya N. Smith, "NebuAd Introduces Next-Generation Online Consumer Privacy Protections, Raising the Bar on Internet Privacy Protection Standards," *Business Wire*, July 8, 2008, accessed May 17, 2013, http://www.businesswire.com/news/home/20080708005383/en/NebuAd-Introduces-Next-Generation-Online-Consumer-Privacy-Protections.

[318] Nate Anderson, "NebuAd CEO defends web tracking, tells Congress its legal," *Ars Technica,* July 9, 2008, accessed March 2, 2013, http://arstechnica.com/tech-policy/2008/07/nebuad-ceo-defends-web-tracking-tells-congress-its-legal/.

[319] Andreas Kuhn and Milton Mueller, "Profiling the Profilers: Deep Packet Inspection for Behavioural Advertising in Europe and the United States," *SSRN*, September 1, 2012, accessed March 1, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181. Pp. 23.

have broadened the focus of our business but continue to enhance our technologies for that ISP channel."[320]

As noted previously, Senator Markey sparked off government interest in NebuAd with his May 16, 2008 letter. Markey's own interests did not, necessarily, motivate his letters. As a Democrat who is well known as being sympathetic to privacy concerns, civil liberties groups had written to him and called for a hearing into behavioral advertising. A few months after Markey's letter, the Centre for Democracy & Technology (CDT) prepared a memo concerning the basic legality of the NebuAd system. The memo argued that the 'consent' ISPs were acquiring – which largely amounted to changes in terms of service or small text on mailed billing information – was insufficient because advertising systems fell outside of ISPs' "ordinary course" of operations. Consequently, business exceptions did not let ISPs copy data for NebuAd, which would provide the information for NebuAd to modify subscribers' data streams for advertising purposes. Moreover, American courts had asserted that knowledge of the monitoring capability could not be taken to assume that subscribers had consented to the monitoring when agreeing to terms of service. Finally – and, perhaps, most importantly – the CDT memo argued that NebuAd's approach was radically different from other online advertising practices that relied on cookies, such as DoubleClick's business:

> … the Web sites participating in the DoubleClick advertising network were found to be parties to the communications of the Internet users who visited those sites. As parties to the communications, the Web sites could consent to the use of the cookies to collect information about those communications. Here, of course, the ISPs are not parties to the communications being monitored and the interception or disclosure encompasses communications with sites that are not members of the advertising network. Therefore, the source of consent must be the ISP's individual

[320] Janet McGraw (NebuAd) in Ellen Nakashima, "NebuAd Halts Plans For Web Tracking," *Washington Post*, September 4, 2008, accessed February 7, 2013, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html?hpid=sec-tech.

> subscribers, as it would be impossible to obtain consent from every single Web site that every subscriber may conceivably visit.[321]

Subsequent to CDT's memo, Rep. Markey sent another letter, this time to Embarq, in which the Congressman raised a series of questions that were related to the legality of the NebuAd system. He specifically noted that he had questions "regarding the applicability of privacy protections contained in the Communications Act of 1934, the Cable Act of 1984, the Electronic Communications Privacy Act, and other statutes, to such practices."[322] Many of the points of law raised in Markey's letter paralleled those in the CDT's own memo. The public protestations, media reports, and attention from Congressman Markey ultimately led to a hearing before the Senate Commerce Committee concerning the privacy implications of behavioral advertising targeting. Civil advocates, in essence, focused on NebuAd's actions alone as ethically and legally suspect, and they were successful enough in attracting media coverage that government bodies investigated whether NebuAd's practices were themselves problematic.

The Senate Committee saw two major companies agree that a comprehensive federal law to govern privacy would be appropriate. Google and Microsoft acknowledged that they supported such law, as well as improved consumer education and industry regulation. This assertion that self-regulation was appropriate echoed the statements provided by the FTC at the hearing: disclosures of practice should be identified, users should be able to opt-out of tracking, and the aggregated data should be secure and not used in excess of ways stated to consumers. Facebook took the position that its users were sharing information – Facebook wasn't forcing anything from users – and that "ad targeting that shares or sells personal information to advertisers (name, email, other contact oriented information) without user control is fundamentally different from targeting that only gives advertisers the ability to present their ads based on aggregate

---

[321] Center for Democracy & Technology, "An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd system and Other Uses of Internet Traffic Content from ISPs for Behavioural Advertising," *Center for Democracy and Technology*, July 8, 2008, accessed February 6, 2013, https://www.cdt.org/privacy/20080708ISPtraffic.pdf.

[322] Ed Markey, "Key Lawmakers Question Local Provider Over Use of NebuAd Software Without Directly Notifying Customers," *House.gov*, July 14, 2008, accessed February 6, 2013, http://markey.house.gov/press-release/july-15-2008-markey-embarq.

data."[323] All parties distanced their advertising practices from NebuAd's on the basis that they had relations with websites that served their tracking cookies or showed their ads: these companies did not intercept or modify ISP subscribers' data traffic illegally.

CDT, the lone civil advocacy organization that was called upon at the Senate Committee, asserted that because ISPs could see the entirety of what subscribers were browsing online, advertising linked with the ISP networks was inherently different from the advertising provided by Google, which was not all-pervasive. Moreover, the organization insisted that self-regulation was insufficient, and it called for additional hearings on ISP behavioral targeting, general privacy laws, enforceable FTC guidelines, and a "do not track" regime.[324]

As a result of the NebuAd case, ISPs backed away from using DPI for advertising purposes. Congress and the Senate alike became aware of the potential commercial applications of the technology and how it could (potentially) infringe on Americans' privacy vis-à-vis the Wiretap act. Moreover, advocates had taken a deliberately narrow track; they targeted NebuAd's system as different from traditional cookie-based advertising (e.g. DoubleClick), which ensured that they could target one version of behavioral advertising without running up against well-financed and deeply entrenched corporate bodies that might have otherwise violently resisted advocates' efforts. The FTC established self-regulatory principles, and Google and Microsoft alike avoided any strong privacy regulations that substantively inhibited their advertising systems.

Ultimately, civil advocates 'won' insofar as the perceived privacy-infringing systems were removed from the market by political pressure; other large behavioral advertising firms were minimally affected. Civil advocates successfully raised NebuAd's actions as third-party interference with communications and attracted political and media coverage to support their position. They also appealed to institutional environments

---

[323] Chris Kelly (Facebook's Chief Privacy Officer) cited in Dominique R. Shelton and Stephanie Quick, "Online behavioral advertising – summary of Senate Commerce Committee hearing on July 9, 2008 concerning privacy implications of behavioral ad targeting," *Edwards Wildman Palmer LLP*, July 14, 2008, accessed March 4, 2013, http://www.lexology.com/library/detail.aspx?g=7ca7187a-56e2-4224-bd31-46ed7f2d1540.

[324] Dominique R. Shelton and Stephanie Quick, "Online behavioral advertising – summary of Senate Commerce Committee hearing on July 9, 2008 concerning privacy implications of behavioral ad targeting," *Edwards Wildman Palmer LLP*, July 14, 2008, accessed March 4, 2013, http://www.lexology.com/library/detail.aspx?g=7ca7187a-56e2-4224-bd31-46ed7f2d1540.

where NebuAd lacked significant pre-existing power or support; as a technology and policy entrepreneur, the company was vulnerable to the aggressive positions taken by more established actors, and it ultimately lacked the firm support of powerful complementary actors like the ISPs. Although the consequences for NebuAd were significant (it closed its doors in 2009[325]), so were the consequences experienced by the smaller ISPs that had signed up to adopt NebuAd's technologies. Their reputations were damaged, they lost the potential revenue stream that was linked to NebuAd's practices, and they suffered financially by having to defend themselves in the courts.

National Security

Following the terror attacks of September 11, 2001, the Executive branch of the US government authorized heightened surveillance of data communications within, and that went across, American telecommunications networks. In this section I identify key actors and communities, how government institutions have leveraged DPI as part of the national security apparatus, and the relative ineffectiveness so far of opposing actors to moderate the ways in which DPI is used in the service of US national security.

Almost immediately following the attacks on September 11, the National Security Agency (NSA) was authorized to engage in more aggressive surveillance tactics, tactics that included approaching American telecommunications firms to participate in a warrantless wiretapping program.[326] By the end of the year, the program was operational with the Deputy Attorney General receiving Foreign Intelligence Surveillance Act (FISA) applications – which would normally then be sent to the FISA court for approval – with no indication of where the investigative leads used to justify FISA warrants were originating from.[327] FISA warrants are needed to continue surveillance operations within the US following from international monitoring; thus, if someone outside the US was being monitored who then entered the US, a FISA warrant would be needed for the FBI to continue the investigation. Similarly, a warrant is required when international

---

[325] Stacey Higginbotham, "NebuAd Bites the Dust," *Gigaom,* May 19, 2009, accessed February 7, 2009, http://gigaom.com/2009/05/19/nebuad-bites-the-dust/.
[326] James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (Toronto: Free Press, 2006).
[327] Eric Lichtbau, *Bush's Law: The Remaking of American Justice* (New York: First Anchor Books Edition, 2009).

communications are used to ascertain if a US citizen or resident alien can be electronically monitored.

In 2002, Mark Klein learned that the NSA was building a room at AT&T's Folsom Street location. Subsequently "he heard from other AT&T technicians about similar mystery rooms in other cities across the country."[328] In the following year, 2003, he saw the room actually being built; Room 641A exists "in AT&T's San Francisco switching center that grants that agency access to vast amounts of consumer information."[329] Inside are Narus STA 6400 deep packet inspection appliances. STA equipment "is known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for preprogrammed targets."[330] This analytic capability is possible over data networks by investigating the payload of communications data. Dr. Brian Reid, a former scientist at Bell Labs, has noted that the great thing "about the Narus box is that it gives you the freedom to pattern match on anything. So if you don't want to do key words, if you want to do a mixture of IP addresses and who's your ISP and whether it contained the word 'mother' in all caps, it can do that too."[331] In the case of NSA-driven surveillance, analysts believe that the DPI equipment is used to fully capture 'transactional information' (e.g. email addresses, IP addresses, subject lines of email, time messages are sent, etc.)[332] and then selectively capture full data packet flows when certain (unknown) prerequisites are met.[333]

The largest American ISPs have largely been complicit in this surveillance. Qwest is the largest, known, ISP to refuse to comply with the government's surveillance requests, and they so refused based on legal and moral concerns. The significance of AT&T's involvement in the program cannot be overstated; the company has been involved in 'peering' relationships with most of the largest data transit companies that

---

[328] Eric Lichtbau, *Bush's Law: The Remaking of American Justice* (New York: First Anchor Books Edition, 2009).
[329] Stephen Manuel Wolfson, "The NSA, AT&T, and the Secrets of Room 641A," *I/S – A Journal of Law and Policy for the Information Society* 3(3) (2007). Pp. 411-442.
[330] Kline, quoted in James Bamford, *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America* (New York: Doubleday, 2008), 191.
[331] Reid, quoted in James Bamford, *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America* (New York: Doubleday, 2008), 194.
[332] Shane Harris, *The Watchers: The Rise of America's Surveillance State* (New York: The Penguin Group, 2010).
[333] James Bamford, *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America* (New York: Doubleday, 2008). See also: https://publicintelligence.net/binney-nsa-declaration/.

operate in the US. Peering refers to when ISPs have close links to other ISPs' networks, often in the same buildings, to facilitate faster data transit speeds. Specifically, the following companies' data traffic was subject to NSA surveillance because of their peering relationships with AT&T: ConXion, Verio, XP, Genuinty, Qwest, PAIX, Allegiance, Above-net, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSI Net, and MAE West. That these relationships were also subject to surveillance indicated that "AT&T has constructed an extensive—and expensive—collection infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information, *not only for communications to overseas locations, but for purely domestic communications as well*."[334]

Similar to AT&T, Verizon – which predominantly routes domestic communications – established secret rooms and partnered with Verint to receive surveillance equipment. In the case of Verizon, the company would receive "watch-listed names from the NSA" and "then reroute their Internet communications into that room, which is packed with secret Verint machines and software. After passing through the Verint hardware, the messages are then transmitted in real time to a central government surveillance hub in Sterling, Virginia."[335] Other ISPs, including BellSouth (a subsidiary of AT&T), were suspected of being involved in operations paralleling Verizon's. As would be realized much later, although the NSA guaranteed that their surveillance systems would minimally – if at all – capture Americans' email message and phone conversations, this guarantee did not function in practice. An audit of the NSA's logs ultimately revealed significant capture and retention of American communications.[336] On the whole, much of the US ISP community has been complicit in this surveillance. They form a community united in its efforts to avoid punishment for cooperating with the government's programs; moreover, they are united on the basis that they may enjoy

---

[334] Scott Marcus, quoted in James Bamford, *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America* (New York: Doubleday, 2008), 195.
[335] James Bamford, *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America* (New York: Doubleday, 2008).
[336] Kim Zetter, "Former NSA Official Disputes Claims by NSA Chief," *Wired*, July 29, 2013, accessed March 3, 2013, http://www.wired.com/threatlevel/2012/07/binney-on-alexander-and-nsa/.

payment, political capital, or preferred status when applying for Top Secret contracts as a result of their support.[337]

Throughout 2004, there were internal legal disputes between the White House and Department of Justice concerning the legality of the NSA program. The disputes reached an apex when the Acting Attorney General, James Comey, refused to authorize a 45-day extension of the program. In response, White House Counsel Alberto Gonzales and Andrew Card, the president's chief of staff, visited John Ashcroft's, the Attorney General of the United States, hospital bed and tried to get him to authorize the NSA's program. Ashcroft refused, and when Comey arrived at the hospital he again refused to authorize the program. The White House, without authorization, continued the program.[338]

Information about the NSA's program is largely the result of whistleblowers such as Klein, Thomas Drake, William Binney, Edward Snowden, media accounts, and persistent efforts on the part of American civil advocacy groups to ascertain the extent, mission, and purpose of the American intelligence community's actions. These parties form a community that is motivated to understand and stop state surveillance that violates US law and infringes upon Americans' reasonable expectations of privacy. Initial lawsuits were filed against telecommunications firms and the government for illegal surveillance actions. Suits filed by the ACLU accused the government of illicitly conducting surveillance but, on appeal, the suits were dismissed on lack of standing because the "plaintiffs could not prove they had been wiretapped by the government; the surveillance was secret."[339] Other efforts, such as asserting inappropriate surveillance of Islamic charities, saw classified documents being rejected as evidence; though a speech by the FBI Deputy Director that discussed the surveillance gave standing to pursue the case.[340] In the wake of revelations of NSA surveillance by whistleblower Edward Snowden additional suits have been, and will likely continue to be, brought.[341]

---

[337] Tim Scorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (Toronto: Simon & Schuster Paperbacks, 2008).
[338] Susan Landau, *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (Cambridge, Mass.: The MIT Press, 2011), 91.
[339] Susan Landau, *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (Cambridge, Mass.: The MIT Press, 2011), 92.
[340] Electronic Frontier Foundation, "Al Haramain v. Obama," *Electronic Frontier Foundation,* August 29, 2012, accessed March 4, 2013, https://www.eff.org/cases/al-haramain.
[341] American Civil Liberties Union, "ACLU Files Lawsuit Challenging Constitutionality of NSA Phone Spying Program," ACLU website, June 11, 2013, accessed September 7, 2013, https://www.aclu.org/national-

In terms of civil cases, the EFF filed suit against AT&T because of its involvement with illegally surveiling citizens' communication. AT&T "acknowledged that the documents describing the layout and configuration for the secure room were genuine"[342] but, before the case could proceed in depth, the Congress passed the *FISA Amendments Act* in 2008. This law provided retroactive immunity to telecommunications companies that had participated in the NSA program. In the lead-up to the legislation, then-Senator Obama's intelligence adviser, John Brennan, argued that such retroactive law as the "right thing to do." As captured by journalist Shane Harris, Brennan:

> ...knew as well as any of his veteran colleagues that without the telecom companies the intelligence community would be lost on a digital sea. They weren't just a resource. They were partners. They were friends. And you didn't abandon your friends.[343]

To date, no advocacy organization has successfully sued the government to the point of fully revealing the NSA's usage of DPI equipment for domestic or international surveillance activities, though one lawsuit brought by the EFF continues.

Given the ongoing court cases, these communities are still active in opposing the government's actions. The policy network includes epistemic elites who are whistleblowers, ISPs complicit in the surveillance actions, various actors of the US government, and civil advocates. While the whistleblowers have successfully alerted the public of the government's surveillance activities, this has not (seemingly) led to the cessation of the surveillance actions. The NSA's actions are (presumably) continuing on the justification of stopping future terror attacks. It is strongly believed that the NSA's

---

security/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program; Ben Hallman, "NSA Sued By Unusual Coalition Of Gun Rights And Environmental Activists Over 'Dragnet Surveillance'," *Huffington Post*, July 16, 2013, accessed September 7, 2013, http://www.huffingtonpost.com/2013/07/16/nsa-sued-dragnet-surveillance_n_3605104.html?ir=Technology; Mark Clayton, "Snowden leaks give new life to lawsuits challenging NSA surveillance programs," *The Christian Science Monitor*, July 18 2013, accessed September 7, 2013, http://www.csmonitor.com/USA/Justice/2013/0718/Snowden-leaks-give-new-life-to-lawsuits-challenging-NSA-surveillance-programs.

[342] Susan Landau, *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (Cambridge, Mass.: The MIT Press, 2011), 93.

[343] Shane Harris, *The Watchers: The Rise of America's Surveillance State* (New York: The Penguin Group, 2010), 348-9.

understanding of US law has led them to massively collect and algorithmically analyze communications of Americans and foreign nationals.[344] It has also been shown that data has been collected in violation of FISA, with Harris writing that:

> [d]uring a periodic review of surveillance activities officials discovered that the agency had inadvertently collected the phone calls and e-mails of Americans. This was the very "incidental" collection that some had feared. In the course of monitoring supposedly foreign communications, the NSA had trouble distinguishing which phone numbers and e-mail addresses actually belonged to people in the United States. As a result the agency ended up directly targeting Americans without individual warrants – a basic violation of the [FISA] law. [345]

However, the magnitude of the collection of American citizens', residents aliens', and foreigners' personal information may be in excess of Harris' accounts; recent NSA whistleblowers assert that there are extensive database profiles on most American citizens and resident foreign aliens. One whistleblower has publicly stated that:

> Domestically, they're pulling together all the data about virtually every U.S. citizen in the country and assembling that information, building communities that you have relationships with, and knowledge about you; what your activities are; what you're doing. So the government is accumulating that kind of information about every individual person and it's a very dangerous process.[346]

The White House has been a particularly successful actor in the policy network, insofar as it has (seemingly) expanded the auspice of its power without being found to have broken the law, and Congress has yet to repeal the surveillance initiated by

---

[344] BBC News, "Edward Snowden: Leaks that exposed US spy programme," *BBC News*, October 25, 2013, accessed October 29, 2013, http://www.bbc.co.uk/news/world-us-canada-23123964.
[345] Shane Harris, *The Watchers: The Rise of America's Surveillance State* (New York: The Penguin Group, 2010). 355.
[346] William Binney, quoted in Ms. Smith, "HOPE 9: Whistleblower Binney says the NSA has dossiers on nearly every US citizen," *Network World,* July 15, 2012, accessed March 8, 2013, https://www.networkworld.com/community/blog/hope-9-whistleblower-binney-says-nsa-has-dossiers-nearly-every-us-citizen.

President Bush, and continued by President Obama. While many of the government's surveillance operations were, once, mostly within a single policy initiative – the Total Information Awareness program, which sought to include privacy protections in its design to limit access to personal information without clear need – controversy over the program led it to be broken into a host of smaller pieces within the intelligence community.[347] Throughout, the Executive has asserted that any actions it has authorized are to protect Americans, and repeated (and now discredited) briefs to Congressional committees have seen members of the US intelligence community assert that Americans are not deliberately targeted. Moreover, if data about Americans *is* collected, then the administration insists that professionals deal with it in a privacy-protective manner.[348] Safety and security, combined with legal challenges to prevent verifying governmental claims, have been key framing and defensive tactics that the federal government has adopted. While ISPs have suffered reputational harm as a consequence of their involvement, no legal harm has directly fallen on them beyond paying legal fees to defend their actions. That legislation was passed to shield them, arguably, demonstrates that their decision to 'work with' the Executive has ensured their ongoing protection from liability associated with the, at best, questionably legal program. Most have limited public commentary of any involvement with DPI-based national security operations.

Ultimately, the civil advocacy community has been the least successful in advancing its interests thus far: their legal efforts have failed to gain significant traction in the courts and, as a consequence, it remains unclear just how successful they have actually been in limiting this mode of government surveillance. Members of this community have struggled to find a domain from which they can affect change; the media broke the story, which set in motion concern and fear amongst government elites that the program might be shut down, but in subsequent lawsuits, the government has (thus far) protected itself and complicit partners from liability. Within the legislative branch, although Democrats appeared ready to oppose the retroactive immunity, their

---

[347] Shane Harris, *The Watchers: The Rise of America's Surveillance State* (London: Penguin Books).
[348] Adam *Gabbatt*, "'Nobody is listening to your calls': Obama's evolution on NSA surveillance," *The Guardian*, August 8, 2013, accessed October 29, 2013, http://www.theguardian.com/world/2013/aug/09/obama-evolution-nsa-reforms.

political will failed. Most significantly, then-Senator Obama reversed his position to support the surveillance, on grounds that it was needed for state security.

So, in short, the framing of this DPI-based surveillance as linked to American security policy has been successful in orienting the agenda, in terms of there being a problem (terrorism) and security solution (i.e. DPI-facilitated mass surveillance), and in terms of being a part of a larger surveillance strategy. Advocates and judges and legislators who have been mindful of the constitutional implications of this surveillance have, thus far, failed to successfully frame the problem or their proposed solutions in the governmental institutions in a way that has subsequently been actualized by the courts. Advocates have been successful in framing DPI with respect to advertising. Arguably, they have been less so when it comes to secretive government uses of DPI. Thus, civil advocates have been far less successful in framing government and ISPs as villains who have been engaged in mass spying of Americans, and, more to the point, have been unable to hold these parties to account in courts of law.

Conclusion

The American policy network is best characterized as unsettled, and the communities quite often as being in adversarial positions. ISPs succeeded in legally asserting their right to throttle traffic, though they have been less successful in remaining outside of the copyright debates or in advancing DPI-based advertising practices. Consumer and civil advocates have been most successful with regard to blocking advertising-related uses of DPI, though ongoing court cases mean that they continue to contest how DPI is used for national security purposes. Rights holders have enjoyed successes in advancing their own anti-copyright infringement interests. Finally, the government's Executive branch has enjoyed success by pressuring ISPs to voluntarily adopt a 'solution' to copyright infringement and has, to date, been successful in preventing civil rights groups from blocking its warrantless surveillance programs. Throughout the debates, some media organizations have kept abreast of what actors are engaged in and – in the case of national security in particular – been responsible for reporting on events that subsequently spawned the very debates themselves.

The activities of this American policy network have often been fractured on the basis that a series of different arenas have hosted the debates. The fact that these contests have happened at the FCC, the FTC, through Congressional and Senate and Executive levels of government, as well as in the public media has prevented any single party or institution from 'owning' the issue of deep packet inspection. Instead its various practices have been taken up across a range of government institutions. Moreover, the links between these divisions of government are not always tight and, indeed, in the case of the Executive, there have been efforts to *intentionally* keep issues (e.g. copyright) out of the domain of the legislatures.

This fragmentation of arenas has caused American DPI-related issues to be episodic, if often having a similar cast of characters. With network management, the law has ruled on the FCC's relative impotence, but it remains possible – if doubtful – that Congress might enact legislation to clarify the FCC's regulatory powers. Similarly, the copyright issue will now move out of policy circles and towards the public light as individuals begin experiencing the effects of their ISP interfering with their Internet connections because of alleged copyright infringements. It remains unclear what making infringement 'personal' will mean for whether DPI re-emerges as a 'solution' once individuals are incorrectly accused of infringement; it's possible the six-strikes system could collapse under its own weight, and nothing replaces it, or that DPI is brought back onto the agenda as a 'more accurate' means of detecting infringement in contrast to the current (and deficient) practices linked with six-strikes. The 'deadest' issue in the United States seems to be the use of DPI for advertising. Unless a motivated actor chooses to broach the issue again, the network is relatively settled on the inappropriateness of NebuAd-style uses of the technology. Arguably the most 'live' – and longest running – issue in the US revolves around the ongoing litigation concerning the federal government's surveillance operations. With regard to this issue, actors remain in a heated effort to articulate the (il)legality of the government's actions. This issue, however, sees a highly elite and entrenched set of actors mired in conflict. No new policy entrepreneurs seem likely to appear on the horizon any time soon.

So, what can be said, in aggregate, about the American situation? Vendors have largely emerged from the debates unscathed (minus NebuAd). They continue to sell their

equipment to ISPs, universities, and government alike. There has also been significant governmental involvement, with the White House's influence significantly affecting how DPI is taken up. Civil advocates have experienced successes, but those have been relegated to private uses of the technology, where the FCC was not responsible for regulating the technology's use. The FCC's setback has actually turned it into a (generalized) policy entrepreneur on the basis that it must now craft inventive strategies to regulate broadband services under its more limited regulatory mandate. This setback is arguably one of the most significant changes over the past decade, and it speaks to the effectiveness of entrenched industry interests to not just shape, but take control of, the broadband policy agenda more generally. Throughout, the media has paid differing amounts of attention to how and why DPI is used in America; significant awards have been received, and whistleblowers and academics alike have been important in crafting media understandings of the appropriate and inappropriate uses of the technology. To date, however, media has significantly affected only the deployment of DPI with regard to advertising, and neither academics nor whistleblowers have been effective in providing sufficient ammunition to advocates to effectively frame DPI as a problem and thus strike it from the range of tools available to ISPs or government agencies.

In what follows, we will turn to the UK to explore how the debates concerning DPI have emerged there; what has the role of various elements of government been, of advocates, and the ISPs? Emergent from our analysis of the UK issues surrounding DPI, we will compare the politics of DPI across our case studies to ascertain if commonalities or significant variations exist across our cases in order to derive conclusions from those findings.

Chapter 6: The UK Experience

Heated debates about Deep Packet Inspection (DPI) in the United Kingdom (UK) have revolved around privacy. DPI is often characterized as a surveillance technology and various policy actors have struggled to frame the nature of the technology as privacy-neutral or privacy-invasive amongst the policy network and to the general public. Some 'purely technical' uses of the technology seem settled, although most other debate items are alive in one format or another. No policy community sees DPI as a 'done' issue. Instead, conflicts around DPI-related practices remain on all groups' minds.

I begin this chapter by outlining the main actors who have taken an interest in varying aspects of DPI on public telecommunications networks and the general positioning of the relevant policy communities. I next address the various issues surrounding DPI: network management, content control and copyright, advertising, and national security. When examining these issues I address the technical, economic, and political affordances linked to the technology and that are relevant to the UK situation. Each section includes a discussion of the relevant issues, associated actors, and who appears to have been more successful in advancing their issues or arguments. The chapter concludes with a brief summary of the key characteristics in the UK situation.

Introducing the Players

A small policy network is invested in practices related to DPI; communities that are interested in DPI include Internet Service Providers (ISPs), civil rights advocates, some media groups, and a set of government institutions. Members of the policy network have tended to try and frame DPI as either a solution to problems or a problem in itself. Without a doubt, advertising and national security uses of DPI have been the most prominent issues that have been taken up by the UK communities. A host of government institutions have either set the policy arenas or participated in other organizations' arenas; this involvement has prevented any single institution from predominantly 'owning' DPI issues.

As a policy community, ISPs have expressed some degree of interest in DPI. The principal ISPs that have been central to the DPI debates include BT and Virgin, as well as the UK Internet Service Provider Association (ISPA). Given their position of power in

digital networks, ISPs have been at the forefront of the debates about DPI in the UK. These companies have not uniformly adopted DPI for the same ends – not all have trialed it for advertising or copyright detection – and one interview subject insisted that the debates around the technology are still in their infancy.[349]

Vendors have also been an active and highly interested community. While they tend to support using DPI to meet business and government objectives, the specific objectives to be met and possible methods of meeting them vary. This community's members have been polarizing amongst UK policy networks: the marketed capabilities of vendors' products have often provided the basis for contestations about how ISPs are using or want to use DPI. Members of the ISP and vendor communities generally see DPI as offering *solutions* to problems like network management or congestion and as posing *opportunities* for revenue growth or (for one vendor) national security sales.

While ISPs and their vendor partners have expressed interest in the technology for economically driven purposes, other groups have expressed concern over how ISPs deploy the technology. Yahoo!, the BBC, and the Voice on the Net Coalition all raised concerns. These groups contended that ISPs could use DPI to develop business intelligence concerning subscriber uses of competing services or use the technology to prioritize ISPs' own services at the expense of their competitors. This community is incredibly loose; while it shares some common understanding of how DPI could be used to weaken members' economic potential, available evidence does not indicate that its members have a strong collaborative relationship.

The civil advocacy community has been the core community opposed to ISPs' uses of DPI. This community includes members who are drawn from established advocacy groups, for example, Privacy International, Foundation for Information Policy Research, Open Rights Group; newly formed groups, for example, BadPhorm; interested individuals; and academics. These individuals and groups are often tightly linked to members of British universities, with prominent advocates often holding university positions. Given their positions, academics have provided expert advice in the form of dispassionate – and thus trusted – scholarship. Moreover, civil advocates have been joined by the head of W3C, Sir Tim Berners-Lee, who has come out against DPI as "a

[349] Interview with telecommunications consultant, September 18, 2012.

really serious breach of privacy."[350] In addition to civil liberties advocates, consumer advocates have raised worries about how DPI could be deployed, focusing on how consumers might never know that their data traffic is being throttled; thus, they are unable to make informed choices about which services to adopt and why to adopt them. This latter group of advocates have also argued that throttling data traffic could weaken businesses' interests in developing services in or providing services to the UK market. Relatively tight bonds, limited resources and labor pools, and highly savvy efforts to negatively frame DPI to the public and government adjudicators characterize this community. Its members have typically framed DPI as constituting a *problem* for which a solution must be found.

Throughout the course of debates on DPI, the media has been attentive to the technology and its proposed and actual uses. *Slashdot*, *Ars Technica*, *The Register*, and *The Inquirer* – all technology-focused publications – have covered the UK issues. Traditional British media, such as *The Telegraph*, *The Guardian*, and the *BBC* have also covered DPI-related issues. Experts have been somewhat critical of the coverage, however, because the technical discussions have been relatively shallow in the press; as one interviewee said, DPI "has made front page news, but relatively small amounts of information have come out. The transparency of the commercial organizations involved – that's the ISPs and the providers – should be a lot better, and it'd make sense for maybe an international body to investigate what's driving DPI."[351]

The issues related to DPI in the UK have been addressed, in one way or another, by a series of government institutions. When advertising was primary on the agenda, the Information Commissioners Office (ICO), City of London police, Home Office, and EU Commission were drawn into policy contestations around these uses of DPI. The Home Office has been implicated in the debate each time the government has introduced surveillance legislation that relies on DPI to meet its stated legislative aim, and the state telecommunications regulator, Ofcom, has been involved with regard to DPI-based throttling activities. In addition to purely UK institutions, the European Commission has

---

[350] Olivia Solon, "Tim Berners-Lee: deep packet inspection a 'really serious' privacy breach," *Wired UK*, April 18, 2012, accessed May 7, 2013, http://www.wired.co.uk/news/archive/2012-04/18/tim-berners-lee-dpi/viewgallery/283287.

[351] Interview with telecommunications professional, September 21, 2012.

paid some attention to UK uses of the technology. Some of these UK institutions have more-or-less been forced to address DPI-related practices, whereas others have proactively identified the technology as a way to 'solve' a problem or conducted hearings before issues escaped relevant government bodies.

Together, the breadth of the issues taken up in the UK has meant that DPI has appeared in a variety of state policy arenas. The ICO and City of London police can investigate and punish inappropriate or unlawful surveillance of data networks, though the relative strength of the ICO was repeatedly drawn into question over the course of my interviews; one person I interviewed went so far as to say:

> Son, let me tell you this: I mean, if nobody has told you about the Information Commissioner's Office, the Information Commissioners Office is the worst privacy regulator in the world and always has been… ICO has never done anything, really, in any institutional capacity or any capacity through the Commissioner, which has been a significant victory for privacy. Nothing, absolutely nothing, since 1984.[352]

The Home Office has contended with government committees that investigated the appropriateness of proposed surveillance legislation and DPI as the enabling technology for the legislation. In the course of these contentious debates, the Office has been a strong political advocate for DPI as a solution to security challenges, though the Office has routinely faced sceptical parliamentary audiences. Ofcom, the UK telecommunications regulator, has sought to 'get ahead' of DPI as an issue during its network neutrality consultations; its aim has, to date, not been to discipline the ISP community but to establish codes of practice so the community can (largely) govern itself.

In summary, a range of policy communities composes the policy network around DPI in the UK. ISPs form one group and have generally expressed interest in using DPI, though the intended uses of DPI have varied. Vendors have often supported ISPs and government alike in efforts to deploy DPI. The consumer and civil rights community is

[352] Interview with privacy advocate, September 29, 2012.

broadly concerned about how DPI could be used to infringe on UK residents' privacy and threaten businesses' competitive potentials. Throughout the policy debates, government institutions have played critical roles in moderating the formal policy arenas, issues to be taken up, and been key to advancing the debates around traffic management and national security in particular.

The Issues

The actors invested in DPI have focused on how ISPs, their vendor partners, and government can, and cannot, use DPI to monitor, mine, or mediate data traffic. In what follows, I discuss how practices linked to the technology have arisen in the UK by way of the following issues: network management, content control and copyright, advertising, and national security. Issues related to DPI have often focused on what ISPs and their partners should be permitted to do to network traffic as well as the degree to which government should monitor citizens' data traffic for national security purposes. Arguably, the key – and most long-lasting – issues taken up by the policy network have been advertising, which introduced the public and a swathe of government bodies to DPI, and national security, which has been a contested issue between government, civil advocates, and ISPs.

Network Management

Using DPI to address network congestion and prioritize data, for strictly technical reasons, has garnered a relatively muted debate in the UK. Most major ISPs, the telecommunications regulator, Ofcom, and civil advocates recognize that DPI can be used for traffic management purposes. While some actors maintain reservations about whether the technology is necessarily the best or ideal means to regulate traffic, relatively little conflict exists amongst players concerning the use of DPI to ensure that data flows across ISPs' networks.

All major ISPs, including AOL Broadband, BT Retail, O_2, Orange, PlusNet Broadband, Sky, TalkTalk, and Virgin Media[353] used DPI for prioritization purposes as of fall 2012. ISPs target P2P applications though, in the case of BT Retail, the existing

[353] Alissa Cooper, "UK Traffic Management Policies," *Alissa Cooper* (personal website), August 12, 2010, accessed November 7, 2012, http://www.alissacooper.com/2010/08/12/uk-traffic-management-policies/.

throttling systems also negatively affect non-HTTP traffic.[354] In 2008, early uses led civil advocates to draft and send a petition that requested that Downing Street "investigate ISPs oversubscribing on their network and throttling broadband." The call was rejected,[355] perhaps because of a voluntary code of practice that UK ISPs agreed to a month before Downing Street's rejection. This Code of Practice was developed because a recurring and significant variance existed between 'headline' speeds (the broadband throughput rates that were advertised to subscribers) and actual speeds (the broadband throughput that subscribers enjoyed when subscribing to the service). The Code was sanctioned by Ofcom and saw fifty-five ISPs sign it.[356] Paragraph 39 of the Code specifically addressed traffic management:

> Where ISPs apply traffic management and shaping policies, they should publish on their website, in a clear and easily accessible form, information on the restrictions applied. This should include the types of applications, services and protocols that are affected and specific information on peak traffic periods.[357]

Two years later, in 2010, Ofcom held a network neutrality consultation that raised traffic management issues again. During this consultation, ISPs stressed that no evidence supported any claims concerning bad uses of DPI-mediated data throttling, and the ISPA worried that "as consumers and regulators are becoming more aware of traffic management in general, these widely applied practices will be placed under unnecessary control."[358] ISPs readily, and often, asserted that Quality of Service management –

---

[354] Vuze, "Bad ISPs," *Vuze* Wiki, modified as of October 12, 2012, accessed November 8, 2012, http://wiki.vuze.com/w/Bad_ISPs#United_Kingdom.
[355] John Oates, "UK.gov tells throttling petition: Choke on it," *The Register*, July 18, 2008, accessed November 7, 2012, http://www.theregister.co.uk/2008/07/18/epetition_broadband/.
[356] Ofcom, "List of ISPs," *Ofcom*, accessed November 8, 2012, http://stakeholders.Ofcom.org.uk/telecoms/codes-of-practice/broadband-speeds-cop/list-of-isps/.
[357] Ofcom, "Voluntary Code of Practice: Broadband Speeds," *Ofcom*, June 5, 2008, accessed November 8, 2012, http://stakeholders.Ofcom.org.uk/binaries/telecoms/cop/bb/copbb.pdf.
[358] ISPA, "ISPA Response to the Ofcom Traffic Management Discussion Paper," *Ofcom*, issued 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/ISPA.pdf.

throttling – was "in fact, a purely commercial/technical matter."[359] The ISPA supported the positions assumed by its members and argued that

> … overall, the debate needs to change from the perception of traffic management as a de facto negative, to a more neutral or positive characterization: traffic management is fundamentally about enabling lower cost, higher quality services. It is only when traffic management is abused that it may become problematic.[360]

ISPs have sought to depoliticize the throttling of content. Verizon argued that traffic management was unrelated to societal or political issues like free speech. In the company's words, "management policies in the network neutrality context are principally concerned with the way a service is delivered, not with the nature of the actual content of the data carried over the network."[361] One consultant underscored the importance of ISPs' ability to control their networks:

> …deep packet inspection means one thing to the Internet industry in terms of managing their networks or talk of it in terms of traffic management . . . I think ISPs must be able to manage their networks, their architectures, and must be able to know what's going over your network, not in terms of the content of it but what types of traffic, as necessary." The consultant also noted that "certain types of traffic might be non-time sensitive and others are very time sensitive.[362]

Thus, the decision to classify some traffic as requiring priority was grounded on 'technical' reasons. However, BT also has argued that such throttles are *economically*

---

[359] O_2, "Telefónica O2 (UK) Limited Response To: "Traffic Management And 'Net Neutrality'" A Discussion Document," *Ofcom*, issued 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Telef_nica_O2_UK.pdf.
[360] ISPA, "ISPA Response to the Ofcom Traffic Management Discussion Paper," *Ofcom*, issued 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/ISPA.pdf.
[361] Christopher Boam and Vikram Raval (Verizon), "Commons of Verizon Communications In the U.K. Ofcom Public Consultation on "Traffic Management and 'Net Neutrality': a Discussion Document," *Ofcom*, issued June 24, 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Verizon.pdf.
[362] Interview with senior UK telecommunications consultant, September 18, 2012.

efficient. Specifically, the company wrote that "the ability to throttle traffic/protocols associated with non-time critical applications and/or prioritise other traffic/protocols has helped ensure that time-critical applications can flourish despite potential or occasional congestion."[363] So, despite DPI being used by ISPs for 'technical' reasons, one ISP claimed that a happy – also technical! – benefit has been the economic flourishing of applications that otherwise might not have survived.

In support of their customers, vendors selling DPI equipment have argued that DPI technologies are beneficial to ISPs. Detica has noted that the technology facilitates new capital and revenue streams that are needed given increasing usage of broadband.[364] Alcatel-Lucent argued that there is no need to regulate DPI technologies so long as the UK ISP market remains competitive; traffic management should not create market-related problems in the UK market so long as such competition exists.[365] In aggregate, the ISP and vendor communities asserted that DPI was used for apolitical traffic management practices. As such, these companies' practices were addressing technical problems that could be solved only by letting ISPs retain independent control of their network operations. The 'problem' of congestion was 'solved' by way of DPI-based management practices.

Those representing the content industries strongly opposed the ISPs' assertions that throttling was apolitical. Yahoo! recognized DPI as an issue because "knowledge acquired via DPI and used in traffic management could incentivize and inform anti-competitive behaviour."[366] In direct contrast to ISPs, which maintained that traffic management enabled efficient behavior by either increasing the rates charged to content providers or by reducing the need to invest in capital infrastructure, the BBC maintained that throttling raised "a serious risk of inefficiency in the wider market if unconstrained

---

[363] BT, "BT Response to Ofcom Consultation on Traffic Management," *Ofcom*, issued September 9, 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/BT.pdf.

[364] Detica, "Traffic Management and 'net neutrality," *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Detica.pdf.

[365] Alcatel-Lucent, "Traffic Management and 'Net Neutrality': A response from Alcatel-Lucent to the Ofcom consultation," *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/AlcatelLucent.pdf.

[366] Yahoo! UK & Ireland, "Traffic management and 'net neutrality': A discussion document," *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Yahoo.pdf.

traffic management becomes the norm."[367] In public comments, ISPs had argued that the BBC's iPlayer was responsible for generating congestion on ISPs' networks. These comments led the BBC to take an explicit position: the discrimination of content by origin (e.g. Skype, BBC, Google) was absolutely unacceptable, whereas discrimination by application type "may be acceptable in exceptional circumstances for technical reasons to manage the network."[368] Together, these companies insisted that Internet traffic mediation could not be seen as 'just' a technical matter; the fungability of DPI – and targeting of specific content delivery protocols – raised significant business concerns that had to be taken into account.

Consumer groups and advocates were largely sympathetic to over-the-top service and content providers, though these groups cast their arguments more broadly. One advocate asserted that the potential for ISPs to change their management policies at any particular time was problematic because it "likely acts against the pursuit of new innovations using any peer-to-peer technology even those that are designed to be "network-friendly" by limiting their own transfer rates when they detect congestion." Moreover, potential changes establish an unstable platform for development, which inhibits design processes for new products.[369] Another actor, the Open Rights Group (ORG), argued that failing to establish the kinds of traffic management that were impermissible could place the UK at a general competitive disadvantage to the United States and rest of the 'open Internet'. Further, while Ofcom's 2010 consultation focused on whether ex ante regulation was appropriate, ORG asserted that ex ante *principles* could let ISPs avoid problems because they would understand what was, and wasn't, acceptable.[370] Abstract concerns – as opposed to pressing demonstrations of ISPs improper behavior – formed the basis of civil advocates' worries.

---

[367] BBC, "BBC response to Ofcom's discussion document on traffic management and 'net neutrality', *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/BBC.pdf.

[368] BBC, "BBC response to Ofcom's discussion document on traffic management and 'net neutrality', *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/BBC.pdf.

[369] Alissa Cooper, "The Next Tim Berners-Lee: Response to Ofcom Discussion on Traffic Management and Net Neutrality," *Ofcom*, September 9, 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Cooper_A.pdf.

[370] Open Rights Group, "Ofcom Net Neutrality consultation," *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/ORG.pdf.

Ofcom's 2010 consultation focused on traffic management *and* network neutrality. Ofcom launched the consultation on the basis that "[w]hilst traffic management potentially offers some benefits to consumers, there are also concerns that firms could use traffic management anti-competitively. The increasing use of traffic management also raises questions about consumers' awareness and understanding of the impact that traffic management has on their broadband service."[371] It is in light of global regulatory action and discussion around the topic of 'network neutrality' that Ofcom sought comments on the stance it should adopt concerning traffic discrimination and how traffic discrimination should be made transparent to consumers. Emergent from Ofcom's consultations have been Codes of Practice but not findings of wrongdoing.

Members of the policy network have advocated against throttling on the basis that it could threaten Internet services that compete with ISPs' own services, but few have directly opposed using DPI to manage congestion that legitimately exists on ISPs' networks. A government regulator focused on the purpose behind inspecting packets using DPI, saying: ". . . if they're just looking at the protocol, and saying "Right, that's HTTP and we'll allow that packet to go through," whereas something else might be connected to a peer-to-peer network, which is something to manage, perhaps the bandwidth, well that's a different thing to looking inside, you know an HTTP packet, and saying and analyzing the contents for advertising purposes."[372] This position was shared by a senior telecommunications consultant that I interviewed[373] and by a civil society advocate.[374] These positions have ensured that traffic management has been a relatively low-key issue in the UK.

Arguably, ISPs have been most successful in accomplishing their goal of using DPI to 'manage' traffic on their networks so long as their actions are linked to maintaining the network's technical integrity. Only when the use of DPI could unnecessarily affect other businesses or online practices have advocates raised concerns, though one did tell me as "a defensive tool to control information on your network, it has

---

[371] OfCom, "Traffic Management and 'net neutrality': A Discussion Document," *OfCom*, June 24, 2012, accessed November 18, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf.
[372] Interview with UK regulator, September 19, 2012.
[373] Interview senior UK telecommunications consultant, September 18, 2012.
[374] Interview with UK civil rights advocate, September 20, 2012.

benefits, absolutely. But I think there are less intrusive ways of achieving the same aims."[375] Further, members of the government recognize congestion-related uses of DPI as permissible. Instead of a hostile regulator, Ofcom has worked with the ISP policy community to develop Codes of Practice that are amenable to the participants. Self-regulation, on the whole, has been an acceptable middle way for participants insofar as it offers guidance for what might constitute bad action; civil advocates have a bar with which to roughly evaluate ISPs' practices, and ISPs avoid the yoke of direct government regulation.

Copyright and Content Control

Though traffic management has been a somewhat cool issue in the UK, the capacities for DPI appliances to monitor for copyright infringement or to selectively prioritize content have arisen as more contested issues. In particular, Virgin partnered with Detica to test a copyright infringement index(ing) system (CView), and documents filed at an Ofcom consultation saw groups such as the Motion Picture Association argue that ISPs should be permitted to discriminate against infringing content. This same consultation saw discussions over the *control* of content, insofar as ISPs raised the potential for traffic management to affect legal services and non-infringing content moving across ISPs' networks. In what follows I first discuss the contestations around CView and then turn to Ofcom's consulations.

Virgin is most prominently linked DPI-related copyright issues because the company reportedly trialed Detica's 'CView' system. This system measured how much of the data on Virgin's network was prospectively infringing on copyright. The CView system split, that is, copied, data traffic from the ISP network so that consumers did not experience a meaningful effect on the speed at which they accessed Internet services and content. CView was designed to capture only traffic associated with popular peer-to-peer protocols; DPI 'picked off' this traffic for subsequent offline analysis. When data was detected as belonging to a peer-to-peer application, the following information was recorded: encrypted customer identity; type of P2P protocol; content identifier value; file

[375] Interview with UK civil rights advocate, September 20, 2012.

size; time stamp.[376] This information was used to calculate the aggregate amount of copyright infringement that Virgin subscribers were likely engaging in, as well as *what* they were downloading.

Detica insisted that CView did not retain personal information because no way existed to link a subscriber record with the recorded IP address; IP addresses were treated by a "pseudorandom replacement algorithm, while any external IP address is ignored. Key generation for the replacement algorithm is managed automatically by the system, including periodic cycling and redistribution of keys, and keys are never made available outside the device. Once a set of keys for a given time-period have been discarded, the process is irreversible." Keys to generate the replacement were not privy to the ISP, thus preventing the ISP from linking P2P traffic with specific subscribers.[377] This process was meant to defray privacy concerns and, as a result, mitigate concerns that members of the public might have with Virgin's monitoring actions.

Though Virgin's stated aim with CView was to develop analytics about users' network usage, another driver was behind implementing CView. The ISP was negotiating an agreement to make music content available to its subscribers at the same time that the company was reported as trialing the Detica systems.[378] The content companies Virgin was negotiating with may have been attracted to CView on the basis that they "are desperate to protect their interests, understandably, and I suppose deep packet inspection could be a way of finding how people are using the data and being able to track back users who are pirating content."[379] So, for Virgin, the CView system was a solution to the 'problem' of infringement, insofar as its licensing deals may have demanded anti-infringement actions on its network. For Detica, its CView technology resolved a problem that its ISPs – and, by association, content industry – partners were experiencing.

Critiques of the CView system were limited, in part because of the short time Virgin flirted with it. Although popular news articles stated that the ISP was using the

---

[376] Richard Clayton, "What does Detica detect?" *Light Blue Touchpaper*, December 7, 2009, accessed November 11, 2012, http://www.lightbluetouchpaper.org/2009/12/07/what-does-detica-detect/.
[377] Personal correspondence with a Detica representative, September 12, 2009.
[378] Milton Mueller, Andreas Kuehn, and Stephanie Michelle Santoso, "Policing the Network: Using DPI for Copyright Enforcement," *Surveillance and Society* 9(4) (2012), pp. 353-354.
[379] Interview with senior UK telecommunications consultant, September 18, 2012.

technology and personal correspondence with Detica representatives indicated it was being used, Virgin later announced that the system had never actually been deployed.[380] Criticisms of CView emerged from the civil society communities; one technologist, Clive Robertson, focused on the system's technical (in)ability to meet Detica's anonymity and privacy claims,[381] though core advocacy against the system focused on legal questions concerning the interception of subscribers' data traffic. Richard Clayton, a noted security researcher at the University of Cambridge, stated that the

> system does "wire-tapping", that's obvious, but the criminal offence is called "interception" and that is carefully defined within the Regulation of Investigatory Powers Act 2000. I expect that Detica would wish to argue that there is no interception because no content is seen by any humans… however, spitting out the file identifier might in itself be sufficient to infringe. It may take some case law before anyone can say for sure.[382]

Concurring with Clayton's analysis, Alexander Hanff, Privacy International's "Head of Ethical Networks," complained about the system to the European Commission. In response, the EU stated that it would monitor how the technology was used.[383] Ultimately, the stances assumed by civil society focused less on the appropriateness of the infringement index itself and more on how Virgin's actions infringed UK residents' communicative privacy. Detica's efforts to insulate their ISP partner from privacy-related concerns failed insofar as advocates were both highly critical of the system *and* successful in attracting negative media attention towards the proposed surveillance practice. This community identified the CView system itself as a problem in excess of any that it was designed to 'solve'.

---

[380] Austin Moodine, "Virgin trials P2P deep packet snooping," *The Register*, January 21, 2010, accessed November 11, 2012, http://www.theregister.co.uk/2010/01/21/virgin_begins_cview_trials/.
[381] For a listing of these issues, see Clive Robertson's comment to "Update to Virgin Media and Copyright DPI" at http://www.christopher-parsons.com/blog/privacy/update-to-virgin-media-and-copyright-dpi/
[382] Richard Clayton, "What does Detica detect?" *Light Blue Touchpaper*, December 7, 2009, accessed November 11, 2012, http://www.lightbluetouchpaper.org/2009/12/07/what-does-detica-detect/.
[383] BBC, "EU to assess piracy detection software," *BBC*, January 26, 2010, accessed November 10, 2012, http://news.bbc.co.uk/2/hi/8480699.stm.

Though advocates, scholars, and even the European Commissioner focused on CView, it remains unclear whether the DPI practice violates the law. Just days prior to the Commission stating it would monitor CView, *The Register* published a retraction, stating that "[t]his article originally stated that Virgin Media's trial of CView had begun. This was incorrect, the system has not yet been implemented."[384] The CView system subsequently faded away and was (seemingly) not implemented on Virgin's network or any other network in the UK. Consequently, the core arena in which the issue played out was the media; neither the courts or any other UK institutions were forced to address Virgin's actions, and the EU Commission went no further than stating it would monitor the practice.

In addition to the CView situation, public comments by Virgin's CEO and statements that Virgin submitted to Ofcom's consultations to Ofcom's consultations into network neutrality and network management both debated the appropriateness of using DPI to block access to 'unlawful' content or to selectively prioritize some content and services. Virgin's comments were predicated on the BBC's iPlayer content streaming system. Prior to iPlayer's release, ISP executives protested against their companies being transformed into 'dumb pipes', or companies that simply transmitted data packets to and from their subscribers. Virgin Media's CEO, Neil Berkett, stated to the media that "[t]his network neutrality thing is a load of bollocks" and claimed that Virgin was establishing a priority delivery network for companies that paid Virgin's priority delivery fees.[385] The company subsequently retreated from its position; it would "offer content providers deals to upgrade their provisioning if they want to ensure best access to broadband subscribers"[386] The honesty of such statements was called into question when an alleged Virgin employee stated that the company had purchased DPI equipment from Allot for application throttling. Following the employee's clams, Virgin wrote that its policies did

---

[384] Austin Moodine, "Virgin trials P2P deep packet snooping," *The Register*, January 21, 2010, accessed November 11, 2012, http://www.theregister.co.uk/2010/01/21/virgin_begins_cview_trials/.
[385] enigma, "Virgin Media CEO Says Net Neutrality is "A Load of Bollocks," *TorrentFreak*, April 13, 2008, accessed November 8, 2012, http://torrentfreak.com/virgin-media-ceo-says-net-neutrality-is-a-load-of-bollocks-080413/.
[386] Christopher Williams, "Virgin Media mops up CEO's 'boll*cks' outburst," *The Register*, April 15, 2008, accessed November 8, 2012, http://www.theregister.co.uk/2008/04/15/virgin_media_net_neutrality/.

"not discriminate internet traffic by application" and that they had "no plans to do so."[387] However, by years-end the company was using DPI for application throttling.[388]

During Ofcom's 2010 consultation, ISPs raised further concerns when discussing how they could use DPI to charge for content delivery, asserting that DPI let them experiment with novel revenue models. As Vodafone stated, the "ability to charge content providers for priority delivery can increase economic welfare by increasing broadband penetration because it would enable network operators to subsidise access prices for income-constrained or price-sensitive users who currently forgo broadband entirely."[389] For O_2, "[t]he development of new wholesale models where content providers contribute to the costs associated with transport traffic in the operators' networks would incentivize content providers to use the networks more efficiently."[390] Whereas the former suggested that charging content providers facilitated bringing broadband to the masses, the latter suggested that the *real* problem with broadband congestion was that for content providers to 'get it' these providers had to be motivated to use less bandwidth. And the solution was to pay ISPs to encourage such motivation. Together, ISPs asserted that the cost of providing service without additional means of raising revenue constituted a problem to which DPI appliances might be the solution. According to the ISPs, they were victims of content providers (legally) making available content that ISPs' own subscribers wanted to access over the Internet.

During the same 2010 consultation, the Motion Picture Association wrote that "[d]iscrimination between authorized and unauthorized content should not be deemed unfair, just as there is no expectation that unlawful content will be tolerated alongside

---

[387] Christopher Williams, "Virgin Media rubbishes P2P throttling rumours," *The Register*, June 23, 2008, accessed November 8, 2012, http://www.theregister.co.uk/2008/06/23/virgin_media_application_throttling_denial/.

[388] Christopher Williams, "Virgin Media to dump neutrality and target BitTorrent users," *The Register*, December 15, 2008, accessed November 8, 2012, http://www.theregister.co.uk/2008/12/16/virgin_bittorrent/.

[389] Vodafone, "Traffic Management and 'net neutrality'," *Ofcom*, September 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Vodafone.pdf.

[390] O_2, "Telefónica O2 (UK) Limited Response To: "Traffic Management And 'Net Neutrality'" A Discussion Document," *Ofcom*, September 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Telef_nica_O2_UK.pdf.

lawful content in the offline world."[391] In effect, the Association argued that ISPs should be legally permitted to discriminate against 'unlawful' content; therefore, Ofcom and other parties (such as the Information Commissioner or the police) should not see DPI practices like those linked to the CView system as 'interception,' and if such an action was regarded as constituting interception, it should not be seen as *illegal* interception. The attitudes of the Motion Picture Association, however, were strongly countered by the UK Security Services. A leaked 2010 memo revealed that industry groups that were advocating for the use of DPI for copyright enforcement were rebuffed on the basis that such practices could encourage regular citizens to learn how to use encryption technologies in order to evade the DPI-driven surveillance.[392] Such evasions threatened MI5's operational surveillance capacities and, as such, raised the issue of copyright detection to the level of a (potential) national security issue. Here, the problem of copyright infringement was situated against a more widespread social problem: resolving rights holders' problems might amplify terror or serious crime offences. DPI, then, could pose a significant problem to public safety if it was adopted for copyright-related practices.

Civil advocacy groups such as the Open Rights Group warned that decisions to throttle P2P traffic were problematic and that identifying such traffic as 'illegal' gave a "false legitimacy to discrimination against legitimate P2P usage."[393] These concerns resonated with those provided by Yahoo!, the BBC, and other companies during the 2010 consultations into network neutrality, when these actors had warned that DPI could enable anti-competitive behaviors by prioritizing ISPs' service and content offerings over those provided by their (perceived) competitors. In the same 2010 consultations, Consumer Focus warned that consumers would be placed at a disadvantage if ISPs throttled traffic because they would be unable to identify how content was being discriminated against, which would impede their ability to complain about traffic speed.

---

[391] Motion Picture Association, "Submission of comments by the Motion Picture Association (MPA) in response to the Discussion on Traffic Management and "net neutrality"," *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/MPA.pdf.
[392] Richard Mollett, "Digital Economy Bill Weekly Update 11 March 2010," *Craphound*, March 12, 2010, accessed May 13, 2013, http://craphound.com/BPDigitalEconomyBillweeklyminutes.pdf.
[393] Open Rights Group, "Ofcom Net Neutrality consultation," *Open Rights Group*, September 2010, accessed May 12, 2013, http://www.openrightsgroup.org/ourwork/reports/ofcom-net-neutrality-consultation.

Consumers simply would not know whether delays in accessing or sending data were because of congestion, throttling, or a content provision deal between ISPs and content owners. Similarly, consumer groups argued that the potential for ISPs to charge content providers and developers for access to subscribers was "likely to undermine business confidence in developing innovative cutting-edge products that may require long-term investment."[394] These actors rebuffed the position that throttling or prioritizing data traffic was purely a technical issue because of the potential externalities or motivations associated with throttling. As with the security services, civil advocates saw that using DPI for content control or anti-infringement purposes constituted a problem in excess to what ISPs might solve. Consequently, ISPs and rights holders were cast as problem-makers and not problem-solvers.

In the later 2012 consultations, Ofcom wrote that it "is possible that increasing use of over-the-top (OTT) online services which require higher bandwidths (such as the video-streaming services provided by BBC iPlayer, LOVEFiLM, Netflix, and Sky), and growth in the number of connected devices per household, is driving up this increase in [broadband] take-up."[395] Some ISPs, such as Vodafone, asserted that in light of such growth the company's management of data traffic "increases the welfare to society to deliver high-value, time-sensitive packets more quickly than low-value or time-insensitive packets."[396] Here, a valuation was placed on the social value of data based on its susceptibility to jitter and latency, with the provider ascertaining what constitutes 'social value'; the ISP did not consult with public stakeholders about what to prioritize or why. Neither did other UK ISPs that selectively prioritized content and applications.

Ultimately, however, Ofcom avoided regulating how ISPs could manage traffic. The 2010 consultations resulted in a Code of Practice meant to guide ISPs on how to manage subscribers' data traffic, and the report that emerged from Ofcom's 2012 consultations left it to ISPs to police themselves, with a warning that bad behavior could

---

[394] Consumer Focus, "Consumer Focus response to Ofcom's discussion paper on Net neutrality and traffic management," *Consumer Focus*, September 2010, May 12, 2013, http://www.consumerfocus.org.uk/assets/1/files/2009/06/Consumer-Focus-response-to-Ofcom-consultation-on-net-neutrality.pdf.

[395] Ofcom, "Communications Market Report 2012," *Ofcom*, July 18, 2012, accessed November 8, 2012, http://stakeholders.Ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf. Pp. 286.

[396] Vodafone, "Traffic Management and 'net neutrality'," *Ofcom*, September 2010, accessed November 19, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Vodafone.pdf.

lead to regulation. Still, Ofcom has been involved in adjudicating the relationship between rights holders and ISPs, insofar as Ofcom asserted that ISPs were not responsible for blocking websites at the behest of copyright holders. This assertion followed from Ofcom's decision that such behavior would have been an unworkable 'solution' to preventing copyright infringement in the UK.[397] Instead ISPs have been forced to send warning letters to subscribers who have been accused of infringing on rights holders' copyrights,[398] and rights holders have turned to the courts to force UK ISPs to block access to websites accused of either massively hosting infringing content or facilitating access to such content.[399]

To date, the most significant use of DPI to monitor for copyright infringement has been shelved, along with the associated deal(s) that Virgin was developing with rights holders. This decision constituted a loss of potential revenue for Detica, but it isn't clear that there was a 'problem' to 'solve' after the deal between Virgin and rights holders collapsed. The civil advocacy community rallied against CView on the basis that it violated individuals' privacy. This community's concerns were operationalized by arguing that CView violated UK interception laws. Though members have never been forced to 'test' whether CView legally violated UK residents' privacy, they framed the detection process as a violation in the media. As such, this community negatively framed this way of using DPI without having to test the legal validity of their arguments; they have, thus far, been able to predominantly assert their position through extra-legal avenues.

Arguably, rights holders, such as the Motion Picture Association, have been successful in accomplishing their aims: while DPI isn't being used to monitor, stop, or report on copyright infringement, ISPs must contact subscribers when alleged actions of infringement occur and block websites at a courts' ordering. Consequently the 'problem' that rights holders face may be being addressed through non-DPI-related practices. In

---

[397] Ofcom, ""Site Blocking" to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act," *Ofcom*, May 27, 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.

[398] Ofcom, "New measures to protect online copyright and inform consumers," *Ofcom*, June 26, 2012, accessed May 12, 2013, http://media.ofcom.org.uk/2012/06/26/new-measures-to-protect-online-copyright-and-inform-consumers/.

[399] Dave Lee, "Court orders UK ISPs to block more piracy sites," *BBC News*, February 28, 2013, accessed May 12, 2013, http://www.bbc.co.uk/news/technology-21601609.

short, DPI simply may not be the most effective or politically feasible way for rights holders to 'solve' the problem of copyright infringement in the UK. Regardless, members of the content rights industry *have* successfully cast copyright infringement as a problem that demands a solution; it just appears that the solution is not linked to a DPI appliance. Ofcom may also claim 'success' on grounds that its consultations have let the institution generally work with members of the policy network to develop Codes of Practice. As a result, Ofcom has avoided expending political capital to rein in network management practices that ISPs have shown a strong interest in continuing.

Advertising

BT Retail and other ISPs flirted with partnering with an advertising company, Phorm, to monitor and modify subscribers' data traffic using DPI. The intent was to target ISP subscribers with either behavioral advertisements or ones keyed to subscribers' online activities. An exceptionally small group of actors was publicly involved in the contestations around using DPI for advertising. ISPs and their vendor partner were principally in favor of the technology, but civil advocates opposed them. In addition, a diverse range of domestic and transnational governing bodies were drawn into the contestations. The significance of Phorm cannot be overstated; as one senior telecommunications consultant said, Phorm "really raised the issue [of DPI] amongst consumers, civil liberties groups, ISPs, and I suppose the general public."[400] In the following paragraphs, I first briefly outline how Phorm's advertising system worked and then the actors and their efforts to frame DPI-based advertising practices.

Phorm's technology modified data packets before they exited the participating ISPs' networking infrastructure. These modifications enabled data-analysis servers to track Internet subscribers' web browsing habits. In effect, the partner ISPs would reroute users' HTTP (i.e. Web) traffic away from the server they were contacting and direct the traffic through a series of proxy servers that Phorm controlled. After passing through these proxies, subscribers would be delivered to the website that they wanted to visit, but their data traffic had been modified en route for ad tracking and delivery purposes. As such, "users whose ISPs deploy Phorm [would] end up with tracking cookies stored on

[400] Interview with senior UK telecommunications consultant, September 18, 2012.

their machine, one for every website they visit, but with each containing an identical copy of their unique Phorm tracking number."[401]

In addition to the DPI engine that modified data traffic in real time, Phorm's system analyzed the websites that subscribers visited; this analysis included tracking search terms and the text surrounding input boxes. After establishing a profile based on the visited URLs, search terms, top ten words on the page, and passing the Phorm identifier passed through an anonymizer, the 'anonymous' information was sent through a "channel server." This server provided ads on websites that were included in Phorms advertising network.[402] The means by which website server data was intercepted meant that websites also had their communications intercepted. Civil society advocates used this fact to argue that Phorm's system violated the Regulation of Investigatory Powers Act 2000 (RIPA).

Phorm's practices were brought to light in early 2008 following an announced deal between the company and ISPs, including BT Retail, Virgin Media, and Talk Talk Group. Phorm also announced it was "already working with ad agencies and partner websites, including the Financial Times, the Guardian, MySpace and Universal McCann."[403] Phorm and the group of ISPs, in particular, formed a community that was interested in generating revenues based on targeting advertisements to subscribers. When first discussed in 2008, only Talk Talk Group indicated that subscribers would opt-in to the system;[404] internal BT documents suggested that subscribers would have to opt-out, and it wasn't clear which option Virgin would choose.

While the 2008 announcement alone was sufficient to provoke concern amongst some advocates, it was the discovery that BT Retail had secretly trialed the technology between September 23, 2006 and October 6, 2006 that created a furor. The leaked report about the 2006 trials recognized that the "customers who participated in the trial were not made aware of this fact as one of the aims of the validation was not to affect their

---

[401] Richard Clayton, "Stealing Phorm Cookies," *Light Blue Touchpaper*, April 22, 2008, accessed May 10, 2013, http://www.lightbluetouchpaper.org/2008/04/22/stealing-phorm-cookies/.
[402] Roger Clayton, "The Phorm "Webwise" System," updated May 18, 2008, accessed November 6, 2012, http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.
[403] Jemima Kiss, "ISPs sign up to targeted ads deal," *The Guardian*, February 14, 2008, accessed May 10, 2013, http://www.guardian.co.uk/media/2008/feb/14/bt.virginmedia.
[404] BBC News, "Open Rights Group questions Phorm," *BBC News*, March 12, 2008, accessed May 10, 2013, http://news.bbc.co.uk/2/hi/technology/7291637.stm.

experience."[405] BT Retail also recognized that while the opt-out system was technically functional, the company might "need to modify its broadband terms and conditions prior to any deployment. The change must permit BT's broadband network to silently drop cookies on customers' PCs."[406] After the technical report had come to light and been analyzed by the media and civil advocacy groups, BT Retail asserted that "[a]bsolutely no personally identifiable information was processed, stored or disclosed during this trial," a point that one of BT's customers insisted meant that "all my information was processed, stored or disclosed but the personal bits were filtered out." In the face of the outcry, Virgin "sought to publicly clarify" its relationship with Phorm a few months after Phorm's press release had announced the ISP as a corporate partner. Specifically, Virgin wrote that:

> Virgin Media has signed a preliminary agreement with Phorm to understand in more detail how this technology works but we have not yet decided if it will be introduced … Webwise is a technically complex application which could be implemented in a number of different ways and it will be some months before we can confirm if the service will be made available to our customers and if so, how and when it would be deployed.[407]

ISPs were critical in this initiative because Phorm's systems needed to intercept, analyze, and retarget subscribers' data streams to develop a long-term insight into their online movements; ISPs would receive payments for letting Phorm establish its infrastructure within the ISPs' own. Phorm argued that their technology was a 'win' for all parties: advertisers would enjoy greater ad effectiveness, websites would enjoy higher ad revenues, subscribers would enjoy fewer ads and anti-phishing functions. In effect, all

---

[405] BT Retail Technology. (2007). "PageSense External Technical Validation," *Wikileaks*, January 15, 2007, released on Wikileaks June 4, 2008, accessed November 2012, http://wikileaks.org/wiki/British_Telecom_Phorm_PageSense_External_Validation_report. Pp. 4.
[406] BT Retail Technology, "PageSense External Technical Validation," *Wikileaks*, January 15, 2007, released on Wikileaks June 4, 2008, accessed November 2012, http://wikileaks.org/wiki/British_Telecom_Phorm_PageSense_External_Validation_report. Pp. 5.
[407] Virgin Media, quoted in Christopher Williams, "Virgin Media distances itself from Phorm 'adoption' claims," *The Register*, May 1, 2008, accessed May 10, 2013, http://www.theregister.co.uk/2008/05/01/virgin_media_phorm_misleading/.

the involved parties would have problems that they faced 'solved', and all in a 'privacy protective' way.

The civil advocacy community, which included the Open Rights Group, Foundation for Information Policy Research (FIPR), and newer advocacy groups, 'Dephormation,' and 'Notodpi' took note of the BT Retail/Phorm partnership. This community's work was supported by academics and covered in the popular media. Members of this community argued that Phorm's interception and analysis of data traffic violated RIPA. RIPA §1 makes it an offence to intentionally and without lawful authority intercept any communication in the course of transiting a public communications system.[408] Interception occurs when a person modifies or interferes with the system itself, or the transmissions made by means of the system.[409] On the basis of this alleged wrongdoing, civil advocates filed legal briefs[410] and open letters to government outlining why Phorm's system violated UK law,[411] and raised questions of the system's technical capabilities.[412] Members of this community also argued that Phorm was committing fraud by unlawfully processing personal data and might be targeted for "committing wrongs actionable at the suit of website operators such as the Bank of England."[413] Such wrongs were based on the modification of data traffic, which threatened to change the communications that issued from websites to subscribers' computers.

While FIPR took the initial lead in opposing Phorm, other, newer, advocacy groups also campaigned massively against the company. Two websites and associated groups – BadPhorm.com and Notodpi.org – were established to inform individuals about how DPI generally and how Phorm deployed DPI specifically in the UK. The groups shared similar active members in their public online communications. In return, Phorm targeted these two groups, seeking to discredit and undermine their advocacy efforts by

---

[408] UK Government, "Regulation of Investigatory Powers Act," *Legislation.gov.uk*, 2000 c. 23, http://www.legislation.gov.uk/ukpga/2000/23/contents.
[409] UK Government, "Regulation of Investigatory Powers Act," *Legislation.gov.uk*, 2000 c. 23, http://www.legislation.gov.uk/ukpga/2000/23/contents.
[410] Nicholas Bohm, "The Phorm "Webwise" System – a Legal Analysis," *FIPR*, April 23, 2008, accessed May 10, 2013, http://www.fipr.org/080423phormlegal.pdf.
[411] Nicholas Bohm and Richard Clayton, "Open Letter to the Information Commissioner," *FIPR*, March 17, 2008, accessed May 10, 2013, http://www.fipr.org/080317icoletter.html.
[412] Becky Hogge, "The Phorm Storm," *Open Rights Group*, March 12, 2008, accessed May 10, 2013, http://www.openrightsgroup.org/blog/2008/the-phorm-storm.
[413] Nicholas Bohm. (2008). "The Phorm "Webwise" System – a Legal Analysis," *FIPR*, April 23, 2008, accessed November 7, 2012, http://www.fipr.org/080423phormlegal.pdf. Pp. 2.

refusing to communicate directly with them. Phorm also tried to discredit individual advocates by insisting they lacked legitimacy in the advertising and privacy networks, as well as by spreading misinformation that advocates were involved in illegal actions.[414] As part of their discrediting efforts, Phorm created the 'Stop Phoul Play'website, accused one advocate of being a "serial agitator," and stated that Phorm was "the subject of a smear campaign orchestrated by a small but dedicated band of online 'privacy pirates' who appear very determined to harm our company."[415] The organizers of these two smaller groups provided extensive media interviews about behavioral advertising and also picketed BT Retail's annual general meeting over the company's partnership with Phorm. In addition to being one of the protest's organizers, Alex Hanff provided evidence of Phorm's wrongdoing to the London police to see if charges were appropriate.[416] A petition that saw over 10,000 people assert that Phorm's system was privacy invasive[417] was also launched. As a community, civil advocates identified Phorm and BT as 'villains' who were using DPI to power advertising that was more omnipresent than existing online behavioral ads. Simultaneously, the companies would be violating the law by tampering with Internet subscribers' data traffic without their clear and express consent.

Noticeably absent in the protestations against Phorm was one of the UK's premier privacy advocacy groups, Privacy International. Two key members of Privacy International, Simon Davies and Gus Hosein, consulted for Phorm through 80/20 Thinking Limited. The 80/20 Thinking's report noted that the company had "successfully implemented privacy as a key design component" and that the system "quite consciously avoided the processing of personally identifiable information." Though 80/20 Thinking noted the importance of ISPs communicating clearly with their users, how the Phorm

---

[414] Rupert Neate, "Phorm chief labels critics 'serial agitators'," *The Telegraph*, April 28, 2009, accessed May 9, 2013, http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/5232565/Phorm-chief-labels-critics-serial-agitators.html; Christopher Parsons, "Agenda Denial and UK Privacy Advocacy," *Technology, Thoughts, and Trinkets*, January 19, 2011, accessed May 13, 2013, http://www.christopher-parsons.com/agenda-denial-and-uk-privacy-advocacy/.

[415] Darren Waters, "Phorm hoping to stop 'phoul play'," *BBC News*, April 28, 2009, accessed May 10, 2013, http://www.bbc.co.uk/blogs/technology/2009/04/phorm_hoping_to_stop_phoul_pla.html.

[416] John Oates, "Phorm protestors picket BT AGM," *The Register*, July 18, 2008, accessed May 8, 2013, http://www.theregister.co.uk/2008/07/16/bt_phorm_protest/.

[417] Christopher Williams, "FIPR: ICO gives BT 'green light for law breaking' with Phorm," *The Register*, April 8, 2008, accessed May 2, 2013, http://www.theregister.co.uk/2008/04/07/bt_phorm_ico/.

system might be perceived as invasive, and emphasized the need for opt-in consent,[418] the fact that PI's director consulted for – and significantly approved of – the advertising technology was sufficient to force Simon Davies to write extensively to try and deflect criticms and deny any conflict of interest concerning his roles in Privacy International and 80/20 Thinking consultant.[419] Despite his efforts, Privacy International was publicly taken out of any fight against Phorm's practices.

While the Financial Times, the Guardian, MySpace and Universal McCann were among a series of proposed Phorm partners in early 2008, subsequent to public reporting, a series of large companies, including the Wikimedia Foundation[420] and Amazon,[421] publicly declared that they had opted-out of Phorm's advertising system. Though they didn't make public declarations, LiveJournal, mySociety, and Netmums contacted the Open Rights Group to advise the Group that their companies were also opting out of Phorm's system.[422]

In their interviews, FIPR learned that Phorm had sought the Home Office's approval of the advertising system and that the company felt conversations with the Office had gone "exceptionally well" on the basis that the company had sought to "protect data and enhance privacy." Probationally, the Home Office approved of the technology's legality, though it subsequently retreated by saying "[w]e can't comment on the legal position of targeted advertising services. It is up for [sic] the courts to interpret the law."[423] Still, in a Freedom of Information and Access disclosure, the media discovered that the Home Office had offered "informal guidance" to the company, and documents showed the government "asking the firm what it thinks of the advice it is

---

[418] 80/80 Thinking Ltd. (2008). "First Stage (Interim) Privacy Impact Assessment for Phorm Inc.," *The Guardian*, February 10, 2008, accessed November 10, 2012, http://blogs.guardian.co.uk/technology/PhormPIAinterimfinal.pdf.

[419] Simon Davies, "The conflict of interest – our response," *The Guardian*, March 19, 2008, accessed November 10, 2012, http://www.guardian.co.uk/technology/blog/2008/mar/18/phormsreportfrom8020readi.

[420] Brion Vibber, "Wikimedia Foundation opting out of Phorm," *Wikimedia Blog*, April 16, 2009, accessed May 10, 2012, https://blog.wikimedia.org/2009/04/16/wikimedia-opting-out-of-phorm/.

[421] Darren Waters," Amazon blocks Phorm adverts scan," *BBC News*, April 15, 2009, accessed May 10, 2013, http://news.bbc.co.uk/2/hi/technology/7999635.stm.

[422] Darren Waters, "Amazon blocks Phorm adverts scan," *BBC News*, published April 15, 2009, accessed May 10, 2013, http://news.bbc.co.uk/2/hi/technology/7999635.stm.

[423] Christopher Williams, "Home Office defends 'dangerously misleading' Phorm thumbs-up," *The Register*, April 24, 2012, accessed November 10, 2012, http://www.theregister.co.uk/2008/04/24/home_office_phorm_fipr_bt/.

drawing up in relation to behavioral targeted advertising, and making specific reference to Phorm's technology."[424] This led Baroness Sue Miller, Liberal Democrat spokeswoman on Home Affairs, to say that "[a]nything the Home Office now says about Phorm is completely tainted."[425]

Efforts to involve the domestic courts on the basis of possible RIPA violations were rebuffed. One campaigner filed complaints about the technology to City of London police, which questioned BT over its relationship with Phorm[426] but ultimately did not lay charges. Similarly, the Information Commissioner refused to take action against the BT following letters sent to the Commission by FIPR and Open Rights Group; the ICO stated that the Phorm system avoided retaining personal information and applauded the company for reaching out to civil liberties groups and technologists to explain how the advertising system worked. [427] The ICO also ignored charges that the secret enrolment of BT consumers constituted a violation of RIPA, as well as advocates' assertions that for the company's ad system to be legal under RIPA both individual Internet subscribers *and* website owners had to mutually consent to the interception.[428] In response to the Home Office's and ICO's respective unwillingness to bring charges against Phorm or BT, the EU threatened action against the UK. The EU Telecommunications commissioner, Viviane Reding, wrote to the UK government three times, finally stating that she "may have to proceed to formal action if the UK authorities do not provide a satisfactory response to the Commission's concerns on the implementation of European law in the context of the Phorm case."[429] Subsequently, the European Commission referred the case to the European Court of Justice. In response, the UK government amended RIPA by removing inferences to implied consent and establishing "a new sanction against

---

[424] Darren Waters, "Home Office 'colluded with Phorm'," *BBC News*, April 28, 2009, accessed May 10, 2013, http://news.bbc.co.uk/2/hi/technology/8021661.stm.
[425] Darren Waters, "Home Office 'colluded with Phorm'," *BBC News*, April 28, 2009, accessed May 10, 2013, http://news.bbc.co.uk/2/hi/technology/8021661.stm.
[426] Christopher Williams, "Police quiz BT on secret Phorm trials," *The Register*, September 5, 2008, accessed May 9, 2013, http://www.theregister.co.uk/2008/09/05/bt_phorm_police_meeting/.
[427] Information Commissioners Office," Phorm Advertising – ICO Statement," *Information Commissioner's Office*, April 4, 2008, accessed May 1, 2013, http://www.ico.org.uk/upload/documents/pressreleases/2008/new_phorm_statement_040408.pdf.
[428] Christopher Williams, "FIPR: ICO gives BT 'green light for law breaking' with Phorm," *The Register*, April 7, 2008, accessed May 2, 2013, http://www.theregister.co.uk/2008/04/07/bt_phorm_ico/.
[429] Christopher Williams, "EU threatens 'formal action' against UK.gov on Phorm," *The Register*, February 11, 2009, accessed May 2, 2013, http://www.theregister.co.uk/2009/02/11/phorm_eu_action_threat/.

unlawful interception and breaches of confidentiality in electronic communications, which previously fell outside the scope of RIPA." After implementing these changes, the Commission dismissed its case.[430]

Campaigners also approached the Crown Prosecution Service with evidence of alleged wrongdoing under RIPA, though the Service decided that "the available evidence is insufficient to provide a realistic prospect of conviction" and "a prosecution would not be in the public interest." Given that Phorm and BT had sought counsel to address RIPA concerns, approached the Home Office, and halted trials after conflicting advice on RIPA permissibility had been received, combined with the Information Commissioner's conclusion that there was no evidence that individuals were negatively affected, the Crown Service declined to prosecute.[431]

Ultimately, the efforts of ISPs and Phorm to justify the DPI-based advertising practices and to rebuff civil campaigners' assertions that such practices were privacy invasive were unsuccessful despite the sympathetic leanings of the ICO, Home Office, and unwillingness of the Crown to prosecute. In effect, ISPs and Phorm could not identify a 'problem' that the advertising system 'solved' *and* establish a community of actors to rebuff civil advocates' identification of the DPI-based advertising system as a problem in itself. Privacy, and, in particular, the potential violation of RIPA served as the primary lines of critique. As one advocate told me, the "primary function of DPI, as a surveillance tool, is to do exactly that; to provide high amounts of information on people's private data usually as part of a nation-wide deployment."[432] So, in casting Phorm's system as a surveillance product, it fell to ISPs and their partners to justify their practices. Given that Phorm retreated from the UK market, its ISP partners abandoned the technology, and the UK government amended the law to preclude practices like Phorm's and BT's, it is safe to say that these corporate actors failed to adequately justify their practices.

---

[430] Jennifer Baker, "EU drops ePrivacy case against UK government," *Computer World UK*, published January 26, 2012, accessed May 2, 2013, http://www.computerworlduk.com/news/public-sector/3332941/eu-drops-eprivacy-case-against-uk-government/.

[431] The Crown Prosecution Service, "CPS decides no prosecution of BT and Phorm for alleged interception of browser data," *The blog of the Crown Prosecution Service*, April 8, 2011, accessed May 7, 2013, http://blog.cps.gov.uk/2011/04/no-prosecution-of-bt-and-phorm-for-alleged-interception-of-browsing-data.html.

[432] Interview with UK civil rights advocate, September 20, 2012.

As noted by one telecommunications professional, the Phorm debacle "changed attitudes within ISPs, very much so, given that the feeling now is that behavioral advertising through that method is a complete no-no. It's not illegal, it's just that consumers would not accept it . . . I think Phorm was an important test case with regard to public feeling as well as legality."[433] While UK ISPs initially may have seen DPI-based advertising as a profitable revenue stream, this is less the case today because customers are "aware of data protection issues" and this debate "parallels the debate around deep packet inspection; what's acceptable, what's not acceptable."[434] One government official said that the notion of consenting to such data inspection for advertising purposes has to extend beyond a private notice; it "isn't about hiding something in page seventeen of your terms and conditions."[435] Any future move towards DPI-facilitated advertising, then, will presumably depend on explicit engagements with the public and advocates, and not on secret trials, subtle changes to legalese, and protracted public relations campaigns that attack civil advocates.

National Security

The prospect of using DPI to meet national security objectives has been a polarizing issue in the UK since 2008, when the Home Office proposed using the technology in the Internet Modernisation Programme (IMP). DPI returned to the agenda in the form of the Communications Data Bill (CDB) in 2012 (which was popularly renamed 'The Snoopers Charter'). Although the CDB was recently withdrawn, it is unclear whether the Home Office is genuinely retreating from proposals associated with these legislative efforts. In what follows, I first summarize the key aspects of IMP and CDB and then identify the actors and policy communities that have been involved in challenging and supporting the surveillance legislation.

IMP was introduced to the public in 2008 (though never formally tabled as legislation) and was meant to "maintain the UK's Lawful Intercept and Communications Data capabilities in the changing communications environment."[436] The Programme was

---

[433] Interview with UK telecommunications professional, September 21, 2012.
[434] Interview with senior UK telecommunications consultant, September 18, 2012.
[435] Interview with UK government official, September 19, 2012.
[436] UK Parliament, "Daily Hansard – Written Answers," *www.parliament.uk*, November 19, 2008, accessed May 12, 2013,

ostensibly focused on "communications data," which the creators identified as "who called whom, when, for how long and from what location."[437] Serious crime was seen as a driving domestic motivation for the enhanced powers, as was updating the law to accommodate the adoption of Internet Protocol-based communications infrastructures. IMP would have required ISPs to monitor data traffic and, in initial proposals, to place collected data into a centralized data store; this requirement was amended in the 2009 so that Communications Service Providers (CSPs) would run databases to hold log data that was specific to their service offerings.[438]

IMP fell away when the government changed to the Conservative Party-Liberal Democratic Coalition, but IMP was replaced with the Communications Capabilities Development Programme (CCDP). The CCDP was subsequently introduced to Parliament in 2012 as the Communications Data Bill (CDB). Under the Bill, landline and mobile ISPs, virtual private network providers, website operators such as Twitter, Google, and blogs, and TOR node operators would be required to retain logs of data communications.[439] Throughout both versions of the legislation, the Home Office was "very keen in winning over ISPs" and was described as "conducting a kind of charm offensive … mostly going on behind closed doors."[440]

The effort to 'win over' ISPs is significant, insofar as executives and advisors of these companies have been sceptical of government proposals. One senior UK telecommunication consultant stated that while law enforcement thinks that having access to more and more data will be helpful, there is a question of whether "the end result provides useful and meaningful information, or there is a danger it could provide inaccurate and therefore it wouldn't be evidential in court."[441] An employee of an ISP told me that "[i]t's not clear if it's the police asking for more powers – they always do

---

http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm081119/text/81119w0032.htm#08112012001081.

[437] The London School of Economic and Political Science, "Briefing on the Interception Modernisation Programme," *LSE,* 2009, accessed November 10, 2012, http://www.statewatch.org/news/2009/jun/uk-lse-briefing-state-interception-prog.pdf.

[438] HC Deb 27 April 2009 c36-7WS referenced by Christopher Williams, "UK.gov to spend £2bn on ISP tracking," *The Register*, April 27, 2009, accessed November 29, 2012, http://www.theregister.co.uk/2009/04/27/imp_consultation/.

[439] Open Rights Group, "Communications Data Bill," *Open Rights Group*, updated May 10, 2013, accessed May 12, 2013, http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill.

[440] Interview with UK telecommunications professional, September 21, 2012.

[441] Interview with senior UK telecommunications consultant, September 18, 2012.

that – or whether the Home Office is actually also trying to enlist them to make it a more credible case."[442] This same person said that "[i]t's almost actually like when the Home Office tries to explain it to the ISPs that they're almost trying to sell the package to the ISPs, to say "OK, we'll give you some recommended suppliers and we'll look after the kit and train up your staff. It's a whole package, and we just want to make it easy for you"."[443]

In advancing the surveillance legislation, the government has sought partnerships with ISPs and a UK firm, Detica. One civil advocate stated that the Draft Data Communications Bill was "the first bit of proposed legislation we've seen that is based on a sales pitch around a specific technology. Which is quite remarkable when you think about it."[444] The advocate was referring directly to Detica's DPI products. A senior UK telecommunications consultant raised their own doubts over whether Detica knew for certain what its equipment is a solution to, because the vendor is deeply involved in marketing uses of DPI to the government and, as such, may be trying to convince government that problems actually do exist.[445]

Civil advocates have formed a policy community arranged against IMP and subsequent surveillance proposals. Throughout their advocacy efforts, they reference an influential report titled "Briefing on the Interception Modernisation Programme," which the London School of Economics (LSE) produced. The Briefing argued that changing technical protocols, multiple communications methods, CSPs' lack of customer knowledge, fragmented service usage, anonymization, data flow internationalization, massive volumes of data in transit, and technically sophisticated cybercriminals were, together, likely to preclude DPI equipment from meeting the government's goals of monitoring criminality online. Encryption and other tools also threatened to limit the efficacy of DPI-based surveillance. One interview subject recognized that with the adoption of communications encryption, it is perhaps better that law enforcement just approach the Googles and Facebooks for data, instead of accessing the traffic over the

[442] Interview with UK telecommunications professional, September 21, 2012.
[443] Interview with UK telecommunications professional, September 21, 2012.
[444] Interview with UK civil rights advocate, September 20, 2012.
[445] Interview with UK civil rights advocate, September 19, 2012.

wire[446] – and the LSE report warned that "finding and identifying the fraction of users of interest to law enforcement and what exactly they are up to, we will still need the police to do policing work. Therefore we should be mindful of the fantasy of solving crimes by merely looking at results from queries across databases."[447]

The Open Rights Group compiled extensive analysis on the proposal,[448] and the group's members, along with other privacy and civil liberties groups, responded to the government's consultation. The report that emerged from the consultation revealed that though there was sympathy for the government's challenge in maintaining order in a digital world, the proposed means of enhancing government powers were opposed.[449] When speaking about the CDB in particular, one advocate said that DPI was "the whole fuckin' thing. I mean, the whole policy is a black box in every single location, just doing DPI, and anything else anyone tells it to do. This is genuinely the first time we've seen policy – legislative proposals – that seem to be coming out of the back of a specific technology."[450] Civil advocates tend to unequivocally oppose using DPI for state surveillance, with one advocate saying: "lawful interception DPI kit I don't think should be allowed to be sold. I think that the power that it gives states or the controllers is just too great. Now is that about DPI itself? No. It's about how someone's grabbed the technology, worked out a market for it, and selling it."[451]

One of the core issues pertaining to the Bill was that CSPs would have to retain or collect information using DPI equipment that was installed in their networks. A problem with the UK government's legislative efforts has focused around explanations of how the technology would collect communications data. One advocate stated,

---

[446] Interview with senior UK telecommunications consultant, September 18, 2012.
[447] The London School of Economic and Political Science, "Briefing on the Interception Modernisation Programme," *LSE,* 2009, accessed November 10, 2012, http://www.statewatch.org/news/2009/jun/uk-lse-briefing-state-interception-prog.pdf.
[448] Open Rights Group, "Communications Data Bill," *Open Rights Group*, updated May 10, 2013, accessed May 12, 2013, http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill.
[449] Home Office, "Protecting the Public in a Changing Communications Environment: Summary of Responses to the 2009 Consultation Paper," *Home Office*, November 2009, accessed May 12, 2013, http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary.
[450] Interview with UK advocate, September 20, 2012.
[451] Interview with UK advocate, September 20, 2012.

> The UK government, for example, argues their use of DPI, should they end up using it, does not warrant an 'interception' of a communications packet, they see it as an extraction. So they're creating new technical terms, saying they will only extract the information that they want from the packets. And they refuse to acknowledge that what they're actually doing is intercepting, analyzing, and then splitting up.[452]

In aggregate, civil rights groups have argued that DPI will not solve the problems that *might* be affecting government. Government legislation is cast as proposing fanciful means of empowering authorities. Moreover, these groups have cast the legislation and accompanying DPI equipment as a disproportionate response to serious crimes enforcement, regardless of the technical efficacy of DPI-based solutions. The problem of government interception, if there is such a problem, is cast as being unsolved by applying DPI to communications networks.

Advocates have been sceptical – and hostile – toward the government's proposals, and committees tasked with evaluating the proposals have joined them. The committees focused on IMP's costs in 2008, asking whether the government could actually implement the programme and, if so, at what financial price? In 2009, they questioned the programme's timeline and technical feasibility. Further, while evaluating the CDB, the committee recalled representatives of the police to explain their justifications for the proposed powers. Several individuals I interviewed doubted that the Home Office or police were effectively making their case to the Committee; the efforts were generally seen as insufficient to convince the committee members that the proposals were sound.

These same interviewees talked about the relative value of civil advocates or members of industry presenting arguments or cases to parliamentary committees; one person said "[t]here are probably about a dozen UK parliamentarians who actually are very knowledgeable about issues. If they're on the committee then obviously the committee's level of knowledge goes up."[453] This said, the committees that discuss DPI are different from others, insofar as the legislation "is such a civil liberties issue that

---

[452] Interview with civil rights advocate, September 20, 2012.
[453] Interview with senior UK telecommunications consultant, September 18, 2012.

we've barely got any politics in it. I mean, we're not talking about the "bloody Tories" or the "weak Lib-Dems" in terms of their positions around this; this is very clearly not a bill that is being proposed by any party – it's being proposed by the security services and the Home Office."[454] If members of parliament lack "technical understanding" of DPI, however, one interviewee stressed that they "don't tend to take very strong positions against DPI."[455] The same interviewee, however, recognized that the government committees that were reviewing uses of DPI at the time of our interview were "getting some of the information" though noted that "their understanding of deep packet inspection doesn't go that deep, still."[456] This having been said, one advocate recognized that the technical complexity of DPI led to challenges in presenting sophisticated arguments to committees, telling me that complexity makes it challenging to underscore what is at stake when debating the technology's uses for state security purposes.[457]

The government committees' concerns have been paralleled by independent bodies. In reference to IMP, with its centralized databases, the ICO warned that "[c]reating huge databases containing personal information is never a risk-free option as it is not possible to fully eliminate the danger that the data will fall into the wrong hands. It is therefore of paramount importance that proposals threatening such intrusion into our lives are fully debated."[458] Ultimately, as cast by successive interviewees, the evaluation of government surveillance proposals at committee hearings is not so politicized that the committees' respective conclusions were obvious from the outset. Instead, the Home Office has failed to make its case as successfully as its opponents have made their own cases.

Against these criticisms, successive governments have argued that these laws and associated powers would implement the European data retention directive in UK law; the directive compels "the providers of publicly available electronic communications services or public communications networks" to retain "certain data, which is generated or processed by them" to ensure that "the data is available for the purpose of the

---

[454] Interview with UK advocate, September 20, 2012.
[455] Interview with UK telecommunications professional, September 21, 2012.
[456] Interview with UK telecommunications professional, September 21, 2012.
[457] Interview with UK civil rights advocate, September 20, 2012.
[458] Information Commissioner's Office, "ICO Statement on the Communications Data Bill," *Information Commissioner's Office*, 20 October 2008, accessed May 12, 2013, http://www.ico.gov.uk/upload/documents/pressreleases/2008/ico_statement_comms_data_bill.pdf.

investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law."[459] Ultimately, in 2009, the Labour government retreated from introducing IMP as legislation without giving a reason, although opposition from ISPs and mobile network companies is believed to have weakened the government's position.[460] The UK government that introduced similar surveillance powers under the Communications Data Bill was a coalition government consisting of the Conservatives and Liberal Democrats. Conflicts between the coalition members were responsible for the Bill going straight to review of the joint committee of lords and members of parliament. Following a report that largely condemned the Bill, the leader of the Liberal Democrats, Nick Clegg, withdrew his party's support of the Bill in April 2013, which effectively killed it.[461] However, despite this revocation of support, the Queen's Speech to parliament in May 2013 included a statement that

> [i]n relation to the problem of matching internet protocol addresses, my Government will bring forward proposals to enable the protection of the public and the investigation of crime in cyberspace.[462]

Advocates, members of the press, and opposition MPs have all come out against proposals to reintroduce broad-based surveillance legislation in light of the Queen's Speech.[463] However, the potential re-reintroduction of these surveillance proposals demonstrate how using DPI for lawful intercept and intelligence gathering remain live issues in the UK.

---

[459] European Parliament and of the Council, "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive," *Official Journal L 105, 13/04/2006 P. 0054 – 0063*.
[460] Christopher Williams, "Mobile networks line up to bash net snooping plan," *The Register*, December 22, 2009, accessed May 13, 2013, http://www.theregister.co.uk/2009/12/22/mobile_imp/.
[461] Alan Travis, Patrick Wintour, and Haroon Siddique, "'Snooper's charter': Clegg kills of Tory hopes of deal on rewritten plan," *The Guardian*, April 26, 2013, accessed May 13, 2013, http://www.guardian.co.uk/world/2013/apr/25/snoopers-charter-nick-clegg-agreement.
[462] Her Majesty Queen Elizabeth II, "The Queen's Speech 2013," UK Parliament, May 8, 2013, accessed May 13, 2013, https://www.gov.uk/government/speeches/the-queens-speech-2013.
[463] Alan Travis, "Queen's speech revives 'snooper's charter' legislation," *The Guardian*, May 8, 2013, accessed May 13, 2013, http://www.guardian.co.uk/politics/2013/may/08/queens-speech-snoopers-charter.

Interviewees in the UK persistently pointed to the role of the European Telecommunications Standards Institute (ETSI) in establishing the conditions for lawful intercept and – by extension – government surveillance capacity in the UK. One subject noted that ETSI was 'captured' by the European security services,[464] another that it was a key place to look to understand how lawful interception equipment must perform in Europe,[465] and yet another that it was "very important" and that it should attract greater attention from civil liberties groups.[466] The links between ETSI and UK national security interests are allegedly quite close; one interview subject noted that the Government Communications Headquarters (GCHQ) and ETSI are trying "to revive the idea of key escrow through identity-based encryption."[467] Such efforts suggest that some arms of the UK government are interested in ensuring that data can be selectively decrypted as it crosses or after it has been intercepted in UK ISPs' networks.

In contrast to worries about ETSI, few saw the International Telecommunication Union's (ITU) report on deep packet inspection as necessarily (re)shaping UK policy, although one person asserted that the ITU "has enormously strong and scary potential, and my impression is you have a lot of third world country representatives wandering around who don't know their technology, and they are easy prey for people who want to manipulate agendas in the ITU and achieve certain policy objectives."[468] In a related vein, a UK government official recognized that a "publication coming out of a reputable organization is, will always have some level of influence, if only because it defines that kind of industry standard."[469] While the ITU's report has recently been released – largely to critique by Western governments, critiques which are based particularly on German concerns that the proposals would standardize decrypting data traffic where DPI equipment retained the decryption keys – its ultimate efficacy in affecting UK policy remains unclear as yet.

To date, advocates, ISPs, and critics of the government surveillance proposals have been largely successful in stymying the use of DPI for policing purposes, though

---

[464] Interview with UK civil rights advocate, September 19, 2012.
[465] Interview with UK civil rights advocate, September 20, 2012.
[466] Interview with UK telecommunications professional, September 21, 2012.
[467] Interview with UK civil rights advocate, September 19, 2012.
[468] Interview with UK civil rights advocate, September 19, 2012.
[469] Interview with UK government official, September 19, 2012.

some remain concerned that DPI is already being used for national security purposes at major UK Internet exchanges.[470] Moreover, the government may ultimately be successful if they introduce explicit surveillance legislation for intelligence *or* policing activities; as noted by one interview subject, the CDB is "usually being seen, or reported in the media, as an intelligence thing. It's not about intelligence gathering, it's not about terrorism; it's about ordinary policy. I mean, if GCHQ aren't doing DPI … they're kinda not doing their jobs properly."[471] Clarity of legislative purposes could let the Home Office more clearly articulate, specifically, the problems to be addressed and how elements of the legislation would go about correcting them.

In the absence of confirmable evidence of such uses, however, it appears that there is a continuing and dedicated effort on the part of the Home Office to implement a DPI-based surveillance regime. At the time of this writing, no conclusion had been reached on the powers associated with the IMP or CDB. The joint committee examining the Bill released their report and government killed the Bill, though at least some facets have (seemingly) been reintroduced in the 2013 Queen's Speech from the throne when opening parliament. Ultimately, however, the contestation around using DPI for national security stems around the (perceived) power it could grant the state, with one advocate telling me "[t]he power it's giving people and the failure for everyone to understand what it's really doing, and not doing, is making a fucking shitshow for us. Is it DPI's fault? Probably not."[472]

Conclusion

DPI has come onto UK policy arenas by way of several core issues. ISPs use the technology to 'solve' traffic management problems and have tried to use it to capitalize on copyright- and advertising-related opportunities. Vendors have not just supported ISPs, but they have acted as central figures in contestations over the technology: Detica, in particular, was a driver behind using the technology for national security and copyright purposes, and Phorm's systems are credited as introducing most members of the UK policy networks to DPI. Consumer and civil advocates have resisted the technology in

[470] Interview with UK civil rights advocate, September 19, 2012.
[471] Interview with UK civil rights advocate, September 20, 2012.
[472] Interview with UK civil rights advocate, September 20, 2012.

most forms, though they have been relatively mute on how the technology is used for traffic management. Rights holders have raised DPI as a possible solution to their own problem – copyright infringement – though prospective RIPA-related problems and MI5's interference have shifted that community's strategies.

This policy network's activities might best be seen as addressing issues in a semi-episodic fashion. A diverse set of government institutions were involved in setting the policy arenas and, as such, no specific institution 'owns' the issue. Instead, different institutions have either taken up or set aside DPI-related practices. The first major episode was the Phorm debacle, when it came to public light in 2008 that secret trials had been conducted years earlier. The second, more limited episode, was CView. In both cases, though civil advocates protested these uses of DPI, no UK government institution could be convinced to bring charges against any involved party. The failure of UK institutions to act led a telecommunications consultant to tell me that while "[l]ots of regulation applies [to DPI]" it's "how you enforce which is the biggest problem."[473] Indeed, Downing Street and the ICO were *supportive* of the Phorm system.

Referring to the government's unwillingness to bring charges against companies that have allegedly used DPI in illegal ways, one telecommunications professional said "[i]n many ways the Commission is seen as a lot stronger on this perhaps than our national regulator" and that, given the EU Commission's attitude towards DPI, "it's fairly clear that doing DPI for business purposes is, needs to be, thought about very carefully."[474] So, the first two major 'episodes' were important in raising awareness of the technology but did not lead to clear legal rules about the (il)legality of using DPI for advertising or copyright detection purposes.

The third episode is composed of a series of smaller elements: national security issues have persisted for five years thus far, and they give no indication of letting up. Successive governments have expressed interest in expanded surveillance legislation that would rely on deep packet inspection though, to date, it remains unclear what *specifically* DPI is meant to 'solve'. Government allegations of needing to 'catch up' to IP-based communications infrastructures have not been met with adequate evidence, and efforts to

[473] Interview with UK telecommunications consultant, September 18, 2012.
[474] Interview with UK telecommunications professional, September 21, 2012.

redefine how systems capture and extract data have been met with scepticism and critique.

Traffic management issues, to date, are barely an episode in their own right. While clearly the policy network has come together to discuss the acceptable ranges of management, major stakeholders generally see this practice as permissible so long as throttling doesn't unnecessarily discriminate against particular content offerings. Of all the issues raised within the UK network, this one is the most 'settled'. Of note, it has been Ofcom that has 'dealt' with this issue, but the institution has a low profile amongst actors. One interviewee best emphasized the general attitude towards the government regulator when they said that Ofcom has had "almost no influence at all" over DPI.[475]

Though members of the policy network often take opposing stances over how DPI can be used, they are all focused on addressing the *practices* linked to DPI instead of whether DPI as a technology should be banned or not. As one civil advocate said to me, "What're we going to do? Ban it? No. That's just not the business we're in…It can exist, you can buy it…There are some technology I see as equivalent to cluster bombs, but DPI is not one of them."[476] However, before these parties can effectively address the issues, they need to define *what* it is that they are contesting. None have the same definition of 'what DPI is': one telecommunications consultant told me that:

> I would say largely, definitions are an issue, because no one really can precisely define what deep packet inspection is, and obviously it means some things to certain people and different things for others.[477]

Even officials who have played a role in explaining DPI internally to the government are hesitant to define it; while "broad definitions" might be assumed, it is the *purpose,* rather than the *action,* of looking at a packet that elicit government intervention.[478] The most positive view of the term was that while DPI is "probably

[475] Interview with UK telecommunications professional, September 21, 2012.
[476] Interview with UK civil rights advocate, September 20, 2012.
[477] Interview with senior UK telecommunications consultant, September 18, 2012.
[478] Interview with UK government official, September 19, 2012.

helpful" it "should be defined more."[479] Partially as a result of the ambiguity associated with the term 'deep packet inspection,' one telecommunications professional recognized that "larger ISPs, they're now thinking of calling it "not so deep inspection" because it's really to detect the character of the traffic rather than the content."[480] The search for a proper definition is leading to entirely new terms.

On the whole, this policy network is characterized by a set of regular actors and communities, with strong variance in the governmental actors who are involved. Though there are some more 'entrenched' actors, such as ISPs and governments, their stature has not meant that they have successfully deployed DPI for their ends. Advocates have been fortunate, insofar as their efforts to negatively frame DPI practices as problems needing a solution have generally been tested only in the court of public opinion. No legal cases have come to completion, and this lack of jurisprudence may be part of what promotes the vibrancy of the UK debates. The UK case is revealing about what happens when a relatively stable group of actors are forced to act across a range of institutions that are differentially empowered, and when policy communities work in non-specialist forums (e.g. the media) to influence domestic behaviors. In the following chapter, I will set the cases against one another to ascertain the comparative insights that can be drawn from them, and, subsequently, conclude by discussing the broader significance of DPI as a prevalent data interdiction technology that is inserted throughout global data networks.

[479] Interview with UK telecommunications professional, September 21, 2012.
[480] Interview with UK telecommunications professional, September 21, 2012.

Chapter 7: What Drives Deep Packet Inspection?

Deep packet inspection and its associated practices have come to public and regulatory agendas in all of the states under study. The Canadian case revealed what happens when a few, fixed government institutions are the primary arenas for debates concerning the technology. In contrast to the Canadian case, the American debates often showed deeply politicized regulators and professional politicians who actively shaped how DPI issues were taken up. Both of these states' engagements with DPI stood in contrast to the UK where weak domestic regulation led the European Union to force the British government to (effectively) forbid certain DPI-based practices. Interestingly, the UK telecom regulator routinely reached conclusions similar to their Canadian and American counterparts when dealing with DPI-related issues.

Significantly, though there were variations in different states' regulatory processes, regulators tended to arrive at common conclusions. Regulatory convergence stands in opposition to the divergence that arose as elected officials entered into the DPI debates: such officials have been guided by domestic politics, and tended to reach significantly different conclusions. In effect, while high-expertise regulatory networks reached common conclusions, elected political officials have demonstrated varying degrees of technical expertise and instead have focused on the politics of communications surveillance. In addition to regulators and elected officials, court systems have also been involved in adjudicating how, when, and under what conditions DPI can be used to mediate data traffic. Effectively, government institutions have served as the primary arenas in which DPI issues are taken up, though the involved government actors often exhibited their own interests in how issues were to be taken up or resolved. The relative role of these different state bodies in the case studies arguably reflects underlying political cultures: whereas regulators are principally involved in the Canadian situation, elected officials and courts play a significant role in the US, whereas the UK has principally seen DPI debates settled by regulators and elected officials.

This chapter examines how each nation has addressed issues related to DPI-based practices. For each issue I briefly outline the variations in institutional decisions made by government across cases, and the extent to which path dependency, international governance, or domestic policy actions explain what has driven DPI for each issue,

recognizing that for any issue a *set* of frameworks as opposed to a single framework might best explain these drivers. Next, I address how participating policy communities have understood DPI differently. While arriving at a common understanding about the nature of the technology might deflate DPI as a term around which issues of communicative privacy, surveillance, and control over packet management orbit, policy actors and the communities they form arguably have their own reasons for intentionally resisting such an understanding. The result is the policy networks in which these debates occur see various players assuming roles derived from their own interests. The chapter concludes by drawing some general lessons about DPI in the policy domains of Canada, the US, and UK, and how surveillance and control technologies and practices have generally unfolded in these jurisdictions. In the concluding chapter I return to the concepts of privacy and surveillance that have pervaded the case studies. Specifically, I argue that the issues linked to deep packet inspection are appropriately regarded as not just a sporadic policy issues but as intrinsically related to the health of democratic states.

Network Management: Commonality through Regulation

The issues that drew DPI-based traffic management practices onto agendas varied in each nation, in part because of the respective countries' telecommunications regulatory frameworks. In Canada, a complaint was brought to the Canadian Radio-Television Telecommunications Commission (CRTC) after Bell Canada used DPI appliances to throttle their wholesale clients' traffic. The subsequent regulatory debates saw most Canadian ISPs argue for the right to use DPI to manage their own subscribers' traffic. The core disagreement between ISPs arose over whether incumbent ISPs could negatively affect their competitor ISPs' data traffic. Members from civil society, consumer groups, and content producers sought to broaden the debate to raise – and resolve – problems concerning how DPI affected retail Internet subscribers' data traffic. The other key federal government institution involved in Canadian traffic management issues was the Office of the Privacy Commissioner of Canada (OPC). The OPC focused on how the technology and ISPs' corporate practices were situated with respect to Canadian privacy law after the Office received a complaint from civil society advocates. Together, the CRTC and OPC largely 'contained' the traffic management issue by issuing decisions restricting how the technology could be used.

In contrast to the Canadian situation, federal regulation in the United States has not required ISPs to 'share' their infrastructure at government-regulated rates. As such, DPI-based traffic management issues arose as telecommunications firms affected their retail subscribers' data traffic. In the case of Comcast's interference with peer-to-peer communications, the primary parties involved were the Federal Communications Commission (FCC), civil society advocacy groups and members of the media, Comcast, and ultimately the federal courts. Civil society advocates raised public awareness about Comcast's actions through media organizations and complained about the actions to the FCC. Ultimately, two very different arenas were involved in managing the issue: the FCC as a high-expertise telecoms arena and the courts as experts on the dimensions of the FCC's regulatory capacity. In this case, the FCC asserted that ISPs could not block access to particular applications and had to notify subscribers of DPI's use, but they could not constrain the policy contest. The courts overturned the FCC's decision and, effectively, reduced the FCC's regulatory power.

Finally, in the UK, Ofcom held open consultations for all parties that were concerned about, or interested in, 'network neutrality'. Ofcom's consultations addressed a broader range of issues than either the Canadian or American instances because of the relative ambiguity of the term, network neutrality. Moreover, the UK debate was not borne out of a specific complaint that launched the UK debate, which stands in contrast to how the issue arose in the other states. Ofcom, like the CRTC and FCC, functioned as a high-expertise telecommunications arena, and out of its consultations emerged Codes of Practice intended to guide ISPs in self-managing their networks as well as to articulate the range of (in)appropriate actions to the broader policy network. Across cases, then, we can say that high-expertise telecommunications arenas functioned as the primary sites through which DPI-based traffic management issues were addressed—only the US showed how the issue 'escaped' the regulator's purview. Further, although the processes by which these institutions took up the issue varied, all of the institutions sought to limit how DPI could be used to manage traffic.

Regulatory Legitimation of Network Management

So, while the prior summary reveals similarities and variances across cases, it doesn't shed light on which theoretical framework(s) help to explain what has driven using DPI

for traffic management or bandwidth throttling purposes. The framework of path dependency suggested that, to date, sunk costs, technical conservatism, and 'small decisions' made at the Internet's inception established key characteristics of the subsequent networks, including empowering the client devices that were attached to the Internet (i.e. the 'ends' of the network) to manage packet transfers, to the detriment of intermediary nodes of the network controlled by ISPs (i.e. the 'core' of the network). That DPI has seen such wide adoption indicates that it 'fit' with existing networking systems; existing technical paths had developed since the inception of the public Internet in such a manner that DPI could be integrated with ISPs networks. The technology's widespread use for traffic management reveals that many ISPs in these states regarded it as a 'natural' next step in alleviating congestion, though the actual 'naturalness' of the adoption is at least partially shrouded based on lack of transparency into ISPs' business decisions. Economic or technical decisions concerning capital investment in network infrastructure that took place over many years may have actually established the conditions that created congestion on data networks, congestion that ISPs posed as the reasons that DPI was needed in the first place. Regardless, given that ISPs have adopted DPI across cases, there has been a certifiable shift in the character of the Internet's routing functionality in these liberal, Western, democratic states. The 'ends' have been forced to cede power, or control over the management of packets, to the ISPs that are running core networking infrastructure. Ultimately, then, we can say that there was sufficient flexibility in the Internet protocols that the 'ends' were overcome by ISPs' actions.

Given that DPI-based traffic management is often identified as a technical solution to a technical problem, it seems reasonable that standards bodies might have played a role in the issue of traffic management. The cases, however, reveal otherwise. The Canadian case civil society advocates argue that IETF standards could address network congestion, but at the same time, one consumer advocate acknowledged "if we say we endorse a standard and there's some part of the standard that's terrible then because you read it kind of … you're scared that you spent two days to read it but don't fully understand it."[481] In addition to some consumer advocates' hesitancy to lean too

[481] Interview with Canadian consumer advocate, January 30, 2012.

heavily on standards, one regulator noted that "[a]s much as possible, we should be able to do our jobs without relying on the minutia of an RFC…I don't think [RFCs] should be influencing beyond it's, it's just another data point."[482] Similarly, a telecommunications executive noted, "[i]n my experience, in front of the CRTC, those kinds of things are not raised very often, and I don't perceive them as being very influential at the CRTC."[483] Though standards were raised in the American case—members of the Electronic Frontier Foundation (EFF) insisted that Comcast's use of RST packets violated IETF standards – they did not play a significant role in how American decisions were ultimately concluded. Similarly, UK actors held that standards bodies were similarly not influential, although one telecommunications consultant did recognize that "[i]n theory they should be influential because RFCs pretty much prohibit DPI, I would say, because something is supposed to be transported from A to B regardless of its content. That is the essential principle…RFCs are the precursors to the policy debates."[484] Ultimately, while some parties were mindful of the role of international standards, the international Internet governance organizations and their associated standards were only minimally influential. These bodies were not used in establishing soft or hard law with regard to using DPI for traffic management in Canada, the US, or the UK, nor did they play a significant role in shaping how government institutions ultimately regulated traffic management practices.

Ultimately, it was the domestic framing of the policy problem, resulting from ISPs' unilateral adoption of DPI, that ultimately governed how DPI could be used. Regulatory bodies that served as policy arenas functioned as high-expertise bodies that were predominantly *recipients* of policy issues. While telecommunications regulators, in each case, may have sought to circumscribe the breadth of issues or to welcome interested policy communities to debate issues in order to establish a commonly agreed upon policy, the regulators themselves tended to react to either direct complaints or agitation in the policy network. Only in the US case could a regulatory body, the FCC, be seen as a strong advocate for its own policy position when, after establishing limits on traffic management practices, the institution had to defend its decision before the courts. Barring this example, governmental institutions did not 'drive' DPI. Instead, non-

[482] Interview with Canadian regulator, February 1, 2012.
[483] Interview with Canadian telecommunications executive, January 31, 2012.
[484] Interview with UK telecommunications professional, September 21, 2012.

governmental and private bodies functioned as the driving actors: regulators subsequently established rules or guidelines that were based on particular domestic regulatory actions, and evidence and arguments provided by the interested policy communities.

In all cases, ISPs defended existing practices that were linked to key elements of their businesses. They framed their use of DPI for managing network congestion as needed to 'keep the packets routing,' whereas other policy communities insisted that such practices threatened emerging markets, businesses, civil and consumer rights, or could not actually address the stated problem of network congestion. The examples that these opposing communities raised were ultimately insufficient to convince regulators that Canadian and UK ISPs' uses of DPI for traffic management should be banned outright. Though Comcast was identified as a villain in the American telecommunications policy arena, the portrayal did not carry over to the legal arena within which network management was ultimately decided. In all cases, regulators were dealing with an issue – traffic management, which had specific technical and practical characteristics – that was actually taking place; in all cases, regulators were being asked to restrict uses of the technology based on how it might be used in the future. In all hearings, ISPs wrote off existing bad practices that were raised by opposing policy communities as technical accidents or legitimate actions against 'bad' protocols or consumers. Though no regulator gave ISPs carte blanche to manage their networks however they saw fit, all decisions acknowledged ISPs' legitimate need and right to manage traffic on their networks, with the caveat that management could not transform the meaning of the content disseminated or received. These regulatory decisions tacitly recognized that some protocols were unduly problematic for ISPs and that regulators were unwilling to block the use of DPI itself in the absence of real, ongoing, and material harm.

Though pre-existing technical and economic paths may have led to DPI's adoption, regulators and courts have affected the capacity for DPI to operate across cases. The result has been that while the technology is still used, its full range of potentialities for traffic management has been delimited. DPI may be seen as part of a continuing lineage of packet inspection and network control appliances, and the deployment of DPI by ISPs may have moved the Internet closer to a point where intermediary nodes enjoy increased packet management capacities. Path dependency explains that the wide scale

adoption of DPI by ISPs constitutes a modification of the network's characteristics in terms of the capacities of network intermediaries that affects the character of the network by rearticulating who controls the management of packets, without affecting the basic functionality of the Internet itself (i.e. endpoints requesting and transmitting packets). However, any account of path dependency only partly explains what has gone on because ISPs' practices have been successfully altered on the basis of the actions undertaken by political actors and in line with the 'flavours' of each state's domestic regulations. Thus, while the technology has set the stage for subsequent conflicts between policy communities and decisions suggest that regulators have ultimately authorized the technological path of the Internet towards heightened intermediary control. Domestic policy advocacy has shaped, moderated, and authorized how the technology is used.

Content Control: Bifurcated Issues and Fragmented Arenas

Significant variation existed in how issues of content control were taken up across cases. The Canadian situation saw policy communities dispute the consequences of using DPI to throttle, or 'manage', peer-to-peer data communications. Such disputes occurred primarily before the CRTC. The conflicts revolved around a core point of whether limiting content dissemination, when such limitations *also* prevented access to content, constituted unfair discrimination towards software developers and content producers who adopted ISP-restricted dissemination systems. In addition to this issue being pursued – twice – by the CRTC, a member of the Canadian parliament raised the issue of DPI being used to discriminate against access to content or communications services. Only the CRTC proceeding produced guidelines to help individuals judge when content was inappropriately rendered inaccessible; this high-expertise institution can reasonably be said to have contained the issue.

In the United States, rights holders identified the core 'problem' that needed resolution. They wanted to stymie access to content that they contended infringed against their copyrights. Policy arenas in which the issue played out included the White House and, to a far lesser extent, the FCC, with the White House functioning as an elite, but not necessarily an expert telecommunications, policy arena for the debate to play out. Moreover, the White House was not neutral on the issue: the Obama administration was reported as engaging in 'arm twisting' to get ISPs to adopt a six-strikes policy that would

apply bandwidth throttling to repeat copyright infringers.[485] If ISPs did not voluntarily agree to the six-strikes system, then they risked potential Congressional involvement.[486] In addition to the White House, the FCC was a relevant policy arena insofar as it asserted that ISPs could not unilaterally block content though, ultimately, the federal court established that such discriminatory action could not be stopped using the FCC's 2005 *Internet Policy Statement*. The US case reveals a division of the 'content control' issue, insofar as the White House process was driven to identify and punish US residents for alleged copyright infringement, and the FCC process focused on whether ISPs could unilaterally prevent access to content or applications.

The UK situation saw public and non-specialist arenas as well as high-expertise regulatory institutions involved in the content and copyright control issues. The media and, to a limited extent, EU Commission were responsible for 'taking on' Virgin's CView copyright-detection system, whereas Ofcom proceedings, in part, evaluated the appropriateness of limiting access to some content. Also, the central government – vis-à-vis its push for the Digital Economy Act – served as another policy arena in which DPI may have been featured, though the possibility of using DPI for copyright enforcement was dismissed subsequent to the UK security services' involvement in the issue. Efforts to identify specific infringements of copyright were ultimately unsuccessful in advancing DPI as a tool to resolve the 'problem' of infringement. However, Ofcom – which presides over the regulatory arena – did agree with the CRTC and FCC positions concerning the (in)appropriateness of blocking access to online content. On the whole, high-expertise telecommunications arenas have played a part in control content and have developed similar policies that are meant to limit ISPs' abilities to unilaterally block or discriminate against applications or data protocols. Arenas not specializing in telecommunications issues have moved away from adopting DPI as a tool-of-choice to address copyright infringement.

---

[485] Nate Anderson, "Major ISPs agree to "six strikes" copyright enforcement plan, *Ars Technica*, July 7, 2011, accessed September 8, 2013, http://arstechnica.com/tech-policy/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan/.

[486] Nate Anderson, "White House: we "win the future" by making ISPs into copyright cops," *Ars Technica*, July 7, 2011, accessed March 4, 2013, http://arstechnica.com/tech-policy/2011/07/white-house-we-win-the-future-by-making-isps-into-copyright-enforcers/; Timothy B. Lee, "ISP flip-flops: why do they now support "six strikes" plan?" *Ars Technica*, July 11, 2011, accessed March 4, 2013, http://arstechnica.com/tech-policy/2011/07/why-did-telcos-flip-flop-and-suport-six-strikes-plan/.

Regulatory Stability Versus Political Uncertainty

Though the prior summary and comparison reveal similarities and differences in how the issue of content control has arisen, these comparisons do not immediately reveal which theoretical frameworks best explain what has driven DPI with regard to copyright and content control. There does not appear to have been significant adoptions of DPI for *fine-grained* control of access to content in any of the case studies. Even though ISPs in all jurisdictions use, or have used, DPI for network management functions in an attempt to control access to content transmitted using 'managed' applications or protocols, little evidence suggests that ISPs have been interested in using DPI to establish control over specific content. Canadian ISPs generally wanted to avoid such control; this avoidance was also publicly true of their American counterparts. Only the UK saw a brief and abortive attempt to use DPI to identify specific content, and this action was linked to a specific ISP's economic interests. While technologies *exist* to enable discrete content control, they have not generally been adopted. ISPs' failure to adopt such technologies suggests that while existing technological paths may be shifting control over packet management away from the edges and to the 'core' of the network, such shifts do not presently include a fine-grained capability to massively filter for specified content for commercial purposes. That there is a distinction between protocol and specific file detection also underscores the fact that the term "deep packet inspection" can obscure how different devices differently act on packet flows. What is good for throttling specific protocols is not necessarily capable of *also* effectively detecting and acting on specific files. Ultimately, wrestling control from the ends may be establishing the technical conditions for enhanced fine-grained control of access to content in the future, though either high-costs (political, economic, or technical) or it being the 'wrong time' for such controls may preclude truly granular commercial control of network traffic in the near future.

None of the cases saw policy communities appeal to international standards bodies with regard to content control. While some communities referred to standards concerning traffic management (as noted in the previous section on traffic management), such standards debates were absent from the more fine-grained oversight of content. Though a recent ITU report did discuss, in part, the regulation of some content flows, the

significance of the report is disputed: one UK civil rights advocate said they "think [DPI] is a domestic issue. I mean, maybe I'm unaware of the politics of how influential that kind of document would be, but no, it's not binding, it has no obligation."[487] Given the (relative) insignificance of these standards organizations, insofar as they do not appear to have been used to launder or justify domestic practices, it suggests that domestic politics primarily drove practices that were linked to content control.

Across all cases, domestic interests and policy debates played a leading role in content control and copyright enforcement politics. Regulatory institutions all avoided issues of discrete monitoring and action against specific content and, given that involved policy communities could not identify such practices as ongoing, those regulatory institutions focused instead on the broader control of content vis-à-vis particular protocols or applications. The result was that ISPs could – and did – argue that any granular discriminations experienced by users of 'problem' applications and protocols were just an externality of ensuring that all subscribers enjoyed fair access to Internet services. In the case of misclassifications, regulators were assured that errors would be corrected after problems were found. Such assurances were successful in diminishing the weight of other policy communities' concerns, insofar as regulators generally took ISPs at their word(s). Regulators uniformly asserted that such externalities should not unduly affect subscribers' online choices for content and maintained that they would act in the face of bad actions and left the matter there. Given that the aforementioned contestations were linked with those surrounding traffic management, regulators all operated as recipients of issues. Though only the CRTC and Ofcom contained the conflict over the issue, Comcast ultimately retreated from its aggressive practices. Together, the regulators established or sought to uphold common policies or principles, but the paths by which they reached their conclusions were steeped in domestic particularities.

Content control has been about more than just the consequence of controlling access to peer-to-peer protocols and applications. Politicians sometimes took interest in the role that telecommunications networks played in transmitting copyright infringing materials at the same time as regulators dealt with the content control issue. The Canadian case saw policy entrepreneurs acting to legislate 'network neutrality' principles

[487] Interview with UK civil rights advocate, September 20, 2012.

in order to prevent unwarranted discrimination against applications and protocols. This case stood in contrast to both the US and UK. Entrepreneurs in the US developed a private system for ISPs and rights holders to act against Internet subscribers who were found to be infringing on copyright; such actions bypassed the Congress and (thus far) the judiciary has not been involved. In contrast, politicians in the UK were involved in discussions about using DPI to enforce policy. Using DPI as a copyright policy instrument was abandoned only because it could have had deleterious consequences for national security policy. Arguably, politicians' stances and positions reflect the political situations in each nation: in Canada, the minority government was hesitant to work across the aisle with a party holding significantly different policy positions and so the issue fell by the wayside. The American approach characterized the dysfunctional Congress, which mandated using non-legislative tactics to get much done. Finally, the UK government revealed what is possible when the government of the day can propose and pass legislation, especially when the government is receptive to the interests of copyright holders.

Ultimately, while a commonality exists across regulatory arenas, the same cannot be said for political arenas. The positions adopted by regulators could be predicted because of their relative stability and access to expertise. The same could not be said of issues that rose to the political agendas. The need to balance outcomes between effective governance of an issue and actually establishing rules that can be agreed to by involved policy communities involved more flexible negotiations, consultations, and means of implementing policy; such balancing acts proved challenging for politicians. In contrast, regulators could appeal to their existing policies and regulations to principally orient any of their decisions. As a consequence, while regulators may have established the rules of the road for ISPs, future political events might drag the issue of using DPI for content control back to the political agenda.

Advertising: The Practice that Never Developed

A significant variation existed between what placed DPI-based behavioural advertising on the Canadian agenda versus that in the United States and United Kingdom. In the Canadian context, concerns were raised in telecommunications regulatory proceedings about how DPI-based advertising could threaten individuals' privacy or undermine

competing advertising markets, but ISPs were not actually using DPI for advertising. As such, the policy communities that raised such concerns were focused on *potential* rather than *existing* applications of the technology. The CRTC proceedings and OPC decision established the permissibility of DPI-based advertising before the practice manifested in Canada. High-expertise government institutions took on the issue without external political interference.[488]

In contrast to the Canadian situation, the American and UK cases revealed situations where companies adopted and deployed DPI for behavioural advertising and subsequently engaged in public policy debates. The United States saw an independent researcher bring NebuAd's actions to light, after which civil society advocates and politicians raised concerns about the company's practices. Congress and courts provided the policy arenas in which NebuAd's practices were addressed; the former arena established elite political arenas that attended less to the technical details of NebuAd's system and more to how ISPs secured subscribers' consent and to questions of the general legality of NebuAd's systems. Court cases will, and have, display different levels of technical acumen as is required to understand the technology for the purposes of applying civil statutes against NebuAd's and their partner ISPs' practices.

In the UK, attention focused on BT's secretive trials of the Phorm advertising system. A host of domestic government institutions were involved, including the Information Commissioner's Office (ICO), Home Office, City of London police, and Crown Prosecution Service, as well as the EU's Telecommunications Commissioner. Domestic institutions were either in favor of the Phorm system (ICO, Home Office) or did not find sufficient evidence of wrongdoing to lay charges (City of London police, Crown Prosecution Service). However, because civil society advocates had a strong understanding of how the technology worked, they could explain that the legality of Phorm's interception and modification of data packets laid bare issues with UK interception law. This expertise was leveraged to the point that the EU Commission took interest in the UK's interception laws, interest that ultimately led the Commission to force the UK government to change that legislation.

---

[488] It should be noted that this policy issue has since re-arisen on the agenda; as of October 2013, Bell Canada is preparing to deploy a behavioral advertising system for mobile and wired Internet communications.

Each of these cases reveals significant variations: the Canada and UK cases show differences between what were considered appropriate practices when domestic regulators first evaluated the issue. This disparity closed, however, when changes to UK interception laws established a consent-based regime regarding DPI-based advertising paralleling that in Canada. Despite regulatory differences, political intervention promoted this common, consent-based doctrine. The US almost exclusively saw elected officials attend to this issue, and they generally came to the conclusion that consent was required for DPI-based advertisement to be regarded as a legitimate business practice. In effect, while regulators reached common ground, it took media attention and civil society advocates' efforts to reach this harmony. The US Congress and Senate responded negatively to NebuAd's actions once alerted to them, and UK institutions altered their position(s) towards Phorm's practices only after the EU Commissioner's involvement. In the end, no predisposition or orientation inherent to the respective government institutions and the associated policy arenas led to the consent-based doctrine: common concerns advocated by civil society advocates ultimately drove a common approach to the practice across cases.

The Successes of Civil Society Advocates

Though the previous summary and analysis of institutions' positions reveal the similarities and differences across cases, these empirical comparisons do not describe how the theoretical frameworks introduced in Chapter Three can explain what has driven DPI. Given that only two of three states adopted the technology for advertising, and given that this technology demands intrusive modifications of packets, it would appear that such modifications constituted an entrepreneurial effort to alter basic 'rules' of the Internet.[489] If adopted, such modifications would have led to the network's core becoming less 'trustworthy' because the ISPs' routing infrastructure would not be involved in just shuttling packets across the Internet. As a result, we can interpret the use of DPI for advertising as having had the potential to establish a new trajectory of the management of packets because private actors would act on captive audiences' (i.e. ISP

[489] Though Bell Canada appears to be adopting behavioral advertising as of October 2013, the company is arguably acting as an entrepreneur, insofar as significant public relations and policy hurdles potentially must be overcome before the practice is regarded as legal, to say nothing of it being normatively acceptable to retail Internet subscribers.

subscribers') communications using "West Coast" code to commercialize those audiences' actions on the Web. Such behaviours would depend on exploiting the generally unencrypted nature of packets exchanged when accessing websites. However, the failure of these practices to take hold speaks to the 'state of the Internet' not being at a juncture where such activities were regarded as appropriate or permissible: Phorm's and NebuAd's technical proposals were not adopted because they stood in opposition to the norms, laws, and principles that govern the transit of Internet packets. Consequently, should DPI for advertising be seen as a potential juncture at which ISPs could have monetized their subscribers' online activities, it was a juncture that has been largely abandoned in the cases under study.[490]

With the exception civil society advocacy groups' references to IETF standards and the technical significance of how DPI could be used to modify packets, the policy communities that took up DPI gave little attention to the ITU, IETF, or W3C. In contrast, domestic policy issues played a significant role in the deployment and repudiation of advertising-based practices. In all cases, non-governmental bodies drove the agenda and government institutions acted as recipients of external disputes. Decisions that the CRTC and OPC reached concerning DPI-based advertising were based on their organizational mandates, past domestic regulatory and legal decisions, and evidence that the participants provided to the domestic contestations. The US and UK saw opposition to the practice based on wiretapping, interception, and consumer law. In all cases, opposition to the practice depended predominantly on applying policies and laws that were already on the books; novel interpretations of existing policies were not needed to show why such advertising practices raised significant legal or privacy concerns. Critically, consumer and civil rights advocates first brought up these arguments: the institutional arenas were ultimately receptive to the arguments, but they did not mandate consent-based approaches on their own.

The means by which existing policies and laws served to rebuff corporate practices varied dramatically across cases, perhaps in part based on the relative entrenchment of the practice. No significant pushback by ISPs happened in Canada, and a

[490] Given that Bell Canada declared it will be conducting behavioral advertising, beginning November 2013, this issue has be re-ignited in Canada. The company's program may (re)test if such advertising is now regarded as permissible, whereas it was not seen as permissible during the initial CRTC hearings.

consensus between parties about what was inappropriate was fairly quick to develop. However, in other cases, there were (failed) attempts to legitimize already-in-operation practices. Such attempts were arguably hindered by two things: first, non-ISP parties were using DPI equipment to modify the payloads of packets. These modifications led to questions about the propriety of these parties, which consumers had never heard of, changing the content of subscribers' communications. Such modifications were blatantly commercial in nature. Second, advertising was out of scope of ISPs' routine business operations. As a result, neither ISPs nor their vendor partners could argue that the advertising practices 'simply' extended previous business behaviours. In effect, ISPs and their advertising partners were policy entrepreneurs and they failed in their efforts. We can generalize from ISPs' experiences with advertising to suggest that companies' controversial new practices can be effectively rebuffed when they almost simultaneously receive media and civil advocacy attention and where those practices bear little relation to pre-existing business practices. Consequently, successful adoption of new programs by ISPs may require a degree of commonality with existing business practices to at least pass an initial cursory analysis by a critical audience.

Ultimately, this comparison across cases reveals that the paths upon which DPI, and ISPs' networks more generally, had not developed sufficiently that DPI-based advertising couldn't be rebuffed. That there were significant changes to practices *after* they had begun reveals that domestic institutions and resistance were significant elements in shaping advertising uses of DPI. Moreover, government generally served as the recipient of issues, insofar as domestic government institutions did not proactively ascertain the validity of the practices. It took pressure from interested policy communities to get government institutions to adjudicate the conditions under which DPI-based behavioural advertising was (in)appropriate.

Policing and National Security: Shrouds of Secrecy

Only when turning to the issue of national security does it appear that government drives the DPI agenda. The Canadian situation has seen successive federal governments try to increase the scope of 'lawful access' powers, though DPI has not explicitly been raised as a way for authorities to access telecommunications information. Canadian telecommunications executives have protested that the technology is not needed to meet

proposed legislative aims; one executive stated that they didn't "believe that the type of technology that's being contemplated in the existing legislation rises to the level of DPI in terms of intrusiveness," but that DPI "is more of a threat to the industry, something that may be imposed externally and the industry would be required to use it."[491] In response to challenges in advancing lawful access legislation through the parliament, the government has moved to friendlier – and more government controlled – policy environments; specifically, updates to government surveillance capabilities have been made in a recent Industry Canada spectrum auction, and the *Solicitor General's Interception Standards* have also been updated behind closed doors. Though there have been changes to *how* telecommunications surveillance occurs in Canada, it remains uncertain what, specifically, these changes constitute.

The Canadian situation can be contrasted with both the American and UK situations. The National Security Agency (NSA) uses DPI as part of its intelligence collection efforts; major American ISPs have participated in surveillance programs that analyze domestic and international Internet traffic. The US situation is characterized by government institutions – including the NSA, White House, and Department of Justice – that are involved in secretly establishing these surveillance programs, with the US Congress having indemnified ISPs for their roles in (potentially) unconstitutional government surveillance. All branches of the US government are implicated in these surveillance practices though it is dubious that politicians are aware of the details of their authorizations: voting for or against NSA powers are the equivalent of asserting a desire to 'protect the homeland' with little consideration given to what the practices of such 'protection' actually entail technically or what the practices mean for US residents' civil liberties.[492]

While the US uses DPI for national security and foreign intelligence purposes it is less evident that the UK government does so. Though successive governments have introduced legislation that would employ DPI for policing, security, and intelligence, the

---

[491] Interview with Canadian telecommunications executive, January 31, 2012.

[492] As an example, Senators Ron Wyden and Mark Udall have persistently argued that government surveillance legislation has been secretly interpreted by government lawyers to authorize mass surveillance activities; save for a select few members of the legislative assembly, members of Congress and the Senate have voted for surveillance legislation without knowing the full implications. See: Charlie Savage, "Senators Say Patriot Act Is Being Misinterpreted," *The New York Times,* May 26, 2011, accessed August 9, 2013, http://www.nytimes.com/2011/05/27/us/27patriot.html.

legislation has been withdrawn each time. The UK scenario is characterized by the government trying to 'get ISPs on side', while civil advocates, parliamentarians, and the mass media have routinely argued that the UK proposal is either unnecessary, overly expensive, impossible to implement, or poses privacy risks. Although the government's surveillance legislation has been repeatedly debated – and rebuffed – some members of the UK policy network expect that the technology is *already* used by national intelligence agencies, and these suppositions are supported by leaked documents that indicate GCHQ is filtering traffic for intelligence purposes.[493] If true, the UK situation would reveal an approach similar to the US, insofar as law would just formally legalize existing practices that may be operating at the edges of, or beyond, current law.

Secret Uses of Surveillance Technologies

While the prior summary of the institutional arrangements across cases reveals variances, it does not shed light on which theoretical framework(s) best explain what has driven DPI for national security and policing purposes. The framework of path dependency suggested that, in part, policymakers might take advantage of technology to affect systems flows by changing the availability of (technologically-based) policy instruments. Placing DPI appliances at major Internet hubs reveals that the government is involved in changing the default 'trusted' nature of the Internet insofar as corporate peering and transatlantic cable landing points are forcibly interlinked with state security equipment. Where such changes transpire and are not refuted or rendered illegal by other aspects of government, then adopting DPI for state surveillance arguably constitutes a novel change to networked infrastructure because the core principles, structures, and associated character of the infrastructure is modified. In such cases, the increased packet management capacities of intermediary nodes is linked to enhancing state-held power to monitor citizens instead of enhancing corporate influence over their subscribers' communications. State adoption of DPI establishes sovereign power over data flows that are seen as transnational in character and thereby asserts state borders around the 'borderless' nature of Internet packet flows. Such assertions might be read as exploiting

[493] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013, accessed June 21, 2013, http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

the 'nature' of Internet standards such that mass, even global, surveillance can be conducted using DPI to parse relevant metadata, communications patterns, and other 'relevant' packet and communications characteristics.

Given that not all states have explicitly adopted DPI for state surveillance purposes, there are clearly other elements guiding its prospective adoption. In turning to international governance institutions, we might expect to see policy laundering vis-à-vis standards, as happened in the IETF in 1999, or attempts to justify domestic behaviours based on decisions or standards established by international governance organizations. At no point in the cases was it suggested that the international governance bodies under study – the ITU, IETF, or W3C – played any role in how Canada, the US, or US use DPI for government surveillance purposes. Similarly, no interviewee mentioned any of these bodies as casting a significant influence on how or why DPI might be adopted or justified for policing or national security purposes. Of note, the European Telecommunications Standards Institute (ETSI) was recognized as a site where *regional* surveillance principles and standards were being developed for European states.[494] In parallel, though not raised by any interviewee, American telecommunications interception requirements have led the FCC, Cable Television Laboratories Inc., and the Alliance for Telecommunications Industry Solutions (ATIS) to all develop lawful interception standards for North American markets.

Variance exists across cases pertaining to how the technology has been adopted for state security, which indicates that domestic politics have principally shaped and driven the technology's adoption. In the US and UK, governments have acted and are acting as aggressive initiators of policy that has faced legal, political, and public scrutiny and outcry. The Canadian case shows how advocates against expanded government surveillance have had the 'advantage' of addressing *proposed* government actions. These advocates managed to successfully concentrate the public and political debates on the ineffectiveness and inappropriateness of such surveillance. These advocacy positions stand in contrast to the situation in the US, where largely confidential interpretations of federal laws have been used to massively expand state surveillance post-9/11.

---

[494] Interview with UK civil rights advocate, September 20, 2012; interview with UK privacy advocate, September 19, 2012.

Government lawyers have routinely invoked state secrecy clauses to prevent the hearing about, or introduction of, evidence about the surveillance programs themselves. The result has been the policy communities opposed to DPI-enhanced surveillance have been stymied in even discussing, let alone stopping, the surveillance. It is possible that revelations of GCHQ's surveillance[495] may lead to similar battles in the UK. While Edward Snowden's revelations concerning NSA and GCHQ surveillance practices have reignited these discussions in both the US and UK, as well as in Canada, it remains to be seen whether courts will restrict national security or foreign intelligence uses of DPI.

Efforts undertaken by network controllers in the cases are predicated on a desire to 'master the Internet', insofar as the explosion of digital communications led intelligence services to analyze, parse, and derive understandings from massive volumes of data. DPI has operated as a key technology to monitor massive swathes of traffic at key Internet exchange points. In the US and UK specific vendors, such as Narus and Detica, have been instrumental in building the equipment needed to conduct this government surveillance. Such efforts to monitor torrents of Internet traffic are part of foreign intelligence services' drive to 'connect the dots' between communications that are potentially related to terrorism, serious crimes, or to actions that are generally detrimental to the 'national interest'. As evidenced in the US and UK, attempts to 'understand' communications links have drawn domestic and international communications alike into security nets, often without the politicians who crafted and authorized surveillance laws knowing how these laws have been exploited.[496] The willingness of executive levels of government and intelligence agencies to establish secret, abstracted, or tortured understandings of these laws for massive, DPI-facilitated surveillance speaks to how both the executives and agencies have shed political oversight in the pursuit of 'keeping the nation safe'. Moreover, the ability to establish and operate these programs underscores the danger of government/corporate collusion, insofar as in the absence of guarantees of government indemnification corporations might resist being

---

[495] See, for example: Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013, accessed Sept 10, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[496] Declan McCullagh, "Senators call for end to Justice Department's 'secret law'," *CNet*, June 11, 2013, accessed August 13, 2013, http://news.cnet.com/8301-13578_3-57588763-38/senators-call-for-end-to-justice-departments-secret-law/.

drawn into these massive surveillance schemes. That the legislative branches of government seem to be routinely failing to hold the executive to account or to let the justice system punish corporations that collude in illegal surveillance, speaks to a damning transition towards a secretive and increasingly authoritarian series of government institutions that are motivated to monitor Internet communications.

Across cases there is an extremely vocal and well-mobilized set of policy communities that are opposed to mass state surveillance. They have been successful in preventing the passage of law in Canada and the UK. However, in response to such opposition, forum shifting has happened in Canada and there have been efforts to legalize secret interpretations of law that have been used to justify mass state surveillance in the US and UK. The politics here are linked to fears about terrorism and serious crime and predicated on the belief that by 'connecting the dots' populations can be kept safe from harm. Despite revelations about the extent of US and UK surveillance, citizens have not risen up against their governments' actions. The refutation or legal opposition to such surveillance practices are left to civil advocacy groups and, to some extent, the courts. In summary, a significant variation exists across what and how government surveillance power has been proposed across cases; despite equal access to the DPI equipment, only the US and (likely) the UK have clearly adopted it. This partial adoption suggests that domestic politics combined with the national security and intelligence gathering potentials of DPI have driven government's adoption of the technology and that international standards bodies have largely been absent in debates about the issue.

Muddled Definitions and Contested Events

The debates concerning deep packet inspection have revealed contestations about what the technology is and what it is for; case studies demonstrated strong disputes within policy communities about the normative, legal, or economic efficacy of some uses of DPI. In what follows, I first contrast how actors and communities have explained what DPI 'is' to reveal differences in how the technology and its associated practices are understood. Throughout the policy contests, the involved communities have, even when using similar terms, held significantly different understandings of how DPI is implicated in broader issues of speech, privacy, and control over communications. To some extent these differences may be the result of ISPs and vendors withholding information about

the full technical capabilities of the equipment. As a result of pre-existing policy differences, combined with different degrees of knowledge regarding specific DPI appliances, issues related to DPI might only be temporarily settled because the regulatory and political conclusions about how the technology can be used do not necessarily coincide with the different political orientations of the interested policy communities. Ultimately, the unsettled nature of DPI itself may be a status that some policy communities want to maintain because it leaves the term as an open signifier for the various issues linked to DPI.

Across the cases, ISPs insisted that they needed DPI to manage their data networks. The Canadian executives saw 'deep packet inspection' as a "kind of blanket term" that was really "a marketing term used to describe various types of equipment which monitor traffic."[497] The technology was often cast as a much needed tool – with engineers reputedly advocating for the technology given an inability to meet data growth given capital plans[498] – and defenses of DPI before the OPC relied heavily on deeply technical discussions of how DPI functioned, what constituted a data packet, and whether DPI practices were associated with subscribers' personally identifiable information. In the case of the CRTC's hearing ISPs filed a great deal of technical information regarding how they used DPI in confidence to the Commission, thus restricting who in the policy network knew what. Though American ISPs similarly referred to the technology as a technical solution to technical problems,[499] it was clearly much more. The technology acted as a locus around which ISPs fought with regulators over how ISPs could independently control and act on their networks. Suggestions that ISPs ought to just transport packets for subscribers were derided, and Verizon explicitly asserted that regulating how ISPs could manage their networks infringed on corporate free speech rights: "Broadband networks are the modern-day microphone by which their owners [e.g. Verizon] engage in First Amendment speech."[500] Members of the UK ISP community were perhaps most sceptical of 'where' the debate concerning DPI was located or what it

[497] Interview with Canadian telecommunications executive, January 31, 2012.
[498] Interview with Canadian telecommunications executive, January 31, 2012.
[499] Comcast, "In the Matter of Broadband Industry Practices – WC Docket No. 07-52," *FCC*, February 12, 2008, accessed June 19, 2013, http://apps.fcc.gov/ecfs/document/view?id=6519840991.
[500] Timothy B. Lee, "Verizon: net neutrality violates our free speech rights," *Ars Technica*, July 3, 2012, accessed June 13, 2013, http://arstechnica.com/tech-policy/2012/07/verizon-net-neutrality-violates-our-free-speech-rights/.

was even about because 'DPI' was seen as an undefined term. On the one hand, the term was seen as "probably" helpful but in need of further specificity; one telecommunications expert stated that they "think it's worth separating out different types of DPI because otherwise there is definitely a degree of conflating very different things."[501] The conflation, here, is between practices: the act of examining packets (and how 'deep') itself is predicated on the *purpose* of such inspection. In effect, the act of inspection alone cannot settle what DPI 'is' for this individual.

This inability to define the term is sometimes seen as confounding policy debates, insofar as "definitions are an issue, because no one really can precisely define what deep packet inspection is, and obviously it means some things to certain people and different things for others."[502] Of note, one UK interviewee regarded the 'definition' of DPI as geographically situated; DPI "means one thing in the States, it means something else in the UK, and it means something else in the rest of Europe…what we need to do is define what is the data and have transparency over the types of data and what conditions under which certain parties will need to interrogate it."[503] The result of these different understandings of the technology and its uses have been contestations over the legitimate practices that ISPs think they can engage in on their own networks, but across cases ISPs commonly regard DPI as a means to take, or retain, control over *their* networks.

ISPs have posed understandings of 'what' DPI is in terms of control over their own property, whereas civil society advocates have often labelled DPI as *inappropriately* influencing or controlling subscribers' communications and actions that happen to pass over ISPs' networks. Canadian civil society advocates regard DPI as "control at the cost of consumer choice" and "as a privacy-invading technology," and one consumer advocate regards the technology as "just like listening to conversations, really." Other Canadian groups, such as those working with disabled Canadians, warned that the technology could discriminate against their members' interests. In this view, DPI is seen as a barrier to the disabled population's ability to access the Internet. In the United States, DPI is "changing the game" by way of "turning an open and innovative platform into just another form of pay-for-play media…When a network provider chooses to install DPI equipment, that

[501] Interview with UK telecommunications professional, September 21, 2012.
[502] Interview with UK telecommunications consultant, September 18, 2012.
[503] Interview with UK telecommunications consultant, September 18, 2012.

provider knowingly arms itself with the capacity to monitor and monetize the Internet in ways that threaten to destroy Net Neutrality and the essential open nature of the Internet."[504] Other groups, such as the EFF, argue that DPI is linked to surveillance of customer data traffic, and that such surveillance is invasive.[505] American technologists who have examined the technology, in particular for its ability to modify data traffic in transit, have described it as an "attack" on subscribers' data connections.[506] UK civil rights advocates use similar descriptions of DPI and refer to DPI as a "black box" that serves "to provide huge amounts of information on people's private data, usually as part of a nation-wide deployment."[507] Another advocate stated that DPI's purpose is threefold, encompassing advertising, copyright, and law enforcement. In aggregate these groups tend to take issue with ISPs examining the application layer of packets and subsequently taking actions based on what is found.

In addition to commercial business and surveillance facets of the technology, DPI is also seen as a security *problem* because it is "actually very, very hard to write a DPI kit that is not itself a massive source of vulnerability."[508] A key issue for civil rights groups in all cases is DPI's reputation for intercepting data traffic, often in surreptitious ways. Richard Clayton, a UK technologist and surveillance expert, regarded actions associated with advertising and copyright detection uses of DPI as involving wiretapping, though he noted that there was room to debate whether such activities necessarily constituted *interception* based on machines – rather than humans – parsing the content.[509] Significantly, however, in no jurisdiction have civil rights or consumer rights advocates fought directly against DPI as a technology itself. A UK advocate summarized the state of things by saying that they couldn't "really think of anyone, anywhere [that's resisted

---

[504] M. Chris Riley and Ben Scott, "Deep Packet Inspection: The end of the Internet as we know it?" *Free Press*, March 2009, accessed July 13, 2013, http://www.freepress.net/sites/default/files/fp-legacy/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf.
[505] Richard Esguerra, "Charter Communications ISPs Halts Traffic Inspection/Advertising Plan," *EFF*, July 25, 2008, accessed June 13, 2013, https://www.eff.org/de/deeplinks/2008/06/charter-communications-isp-halts-traffic-inspectio.
[506] Robert M. Topolski, "NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking," *Free Press* and *Public Knowledge*, June 18, 2008, accessed February 5, 2013, http://www.freepress.net/sites/default/files/fp-legacy/NebuAd_Report.pdf.
[507] Interview with UK civil rights advocate, September 20, 2012.
[508] Interview with UK privacy advocate, September 19, 2012.
[509] Richard Clayton, "What does Detica detect?" *Light Blue Touchpaper*, December 7, 2009, accessed June 23, 2013, http://www.lightbluetouchpaper.org/2009/12/07/what-does-detica-detect/.

the technology]. I suppose one of the difficulties one has is, in fact the main difficulty one has, is what does the public know? And also, what is the media capable of intermediating?"[510] This position was echoed by a Canadian interviewee, who acknowledged "[w]e never did a full campaign against DPI, because once it's in there it's impossible to get rid of."[511] In aggregate, civil and consumer rights policy communities commonly identified surveillance, privacy, content discrimination, and increased commercialization of the Internet as problems that were raised by DPI; for these communities, data 'belonged' to the subscriber, and the subscriber, not their ISPs, should control how the data was read and used.

Within the context of the various policy arenas, other business groups have often raised DPI as a problem or solution, typically without fully characterizing the nature of the technology itself. In Canada, providers such as Google focused on how the technology could enable unjust discrimination between service offerings. Google's position was paralleled by Yahoo! in the UK, when the company acknowledged DPI as an issue because "knowledge acquired via DPI used in traffic management could incentivize and inform anti-competitive behaviour."[512] In a related vein, VoIP companies, like Skype, warned that DPI could be used for anti-competitive purposes, as did content producers and distributers, such as the BBC in the UK and groups representing independent media organizations in Canada. DPI was also seen as a potential threat to Canadian companies that sold adspace online, insofar as DPI-based advertising could closely track subscribers' browsing habits. 'Traditional' online advertising providers, including Google, Microsoft, and Facebook, focused on the legality of their own practices in American proceedings while casting DPI-based advertising companies as engaged in radically different practices.

Companies that were invested in DPI-based advertising practices in the US and UK rejected concerns that their offerings were privacy invasive or that they constituted illegal interception of data traffic; instead, the technologies were recognized as highly

---

[510] Interview with Canadian civil rights advocate, January 30, 2012.
[511] Interview with Canadian civil rights advocate, January 30, 2012.
[512] Yahoo! UK & Ireland, "Traffic management and 'net neutrality': A discussion document," *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Yahoo.pdf.

privacy *protective* and "in compliance with the law."[513] Arguing alongside DPI-based advertising vendors were copyright groups who, in the UK, asserted that the discriminatory capabilities of DPI were 'fair' when it was used to target and block or filter 'unlawful' content. These groups claimed that such online actions were appropriate on the basis that "there is no expectation that unlawful content will be tolerated alongside lawful content in the offline world."[514] Finally, ISPs' most natural allies, their DPI equipment vendors, routinely stressed that DPI did not constitute or lead to anti-competitive or unfair discriminatory practices because market competition would punish ISPs that engaged in such behaviours. Vendors were present in most debates and are important actors by merit of actually producing the equipment that enables ISPs' and governments' DPI-based practices. In aggregate, the range of business interests that took notice of DPI understood it in the following different ways:

- Enabled unjust discrimination of services
- Prevented unjust discriminatory behaviours given competitive telecommunications markets
- Posed risks because DPI lets ISPs derive intelligence about individuals using competing services
- Acted unlike 'traditional' advertising service online
- Operated as a more advanced version of online advertising
- Constituted – or did not constitute – wiretapping
- Functioned as *legitimate* interception and analysis of subscribers' data traffic if used to stymie copyright infringement.

When contrasted against each other, it becomes apparent that these understandings of DPI are tightly linked to particular parties' own interests, though the

[513] Nate Anderson, "NebuAd CEO defends we tracking, tells Congress its legal," *Ars Technica*, July 9, 2008, accessed March 2, 2013, http://www.arstechnica.com/tech-policy/2008/07/nebuad-ceo-defends-web-tracking-tells-congress-its-legal/.

[514] Motion Picture Association, "Submission of comments by the Motion Picture Association (MPA) in response to the Discussion on Traffic Management and "net neutrality," *Ofcom*, September 2010, accessed May 12, 2013, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/MAP.pdf.

focus was again on the appropriateness and implications of ISPs enhancing their control over data coursing across their networks.

Though regulatory institutions have operated predominantly as sites wherein policy debates have occurred, the regulators overseeing these institutions have not been entirely neutral. They have sought to establish limits on the scope of debates as well as to establish or reaffirm regulations over what they are responsible for overseeing. When discussing DPI, one Canadian regulator noted that from "a technical standpoint, strictly, DPI still has a great benefit, I think, but it's been maligned in the industry and the press as being this terrible thing."[515] This regulator regarded DPI as a way to regulate traffic and as having been "there, and telecom operators were worried about being regulated to having dumb pipes, and this was a way for them to monetize their pipes."[516] At the same time, the technology was seen as linked to violations of network neutrality, making DPI, "a problem which results in religious fervour by the masses."[517] The technology is recognized as about more than 'just' network management and telecommunications issues by Canadian officials, however, with the Privacy Commissioner of Canada acknowledging that a "networking technology like deep packet inspection does not stand alone"[518] because such technologies can "look into the content of messages sent over the Internet – enabling third parties to draw inferences about users' personal lives, interests, purchasing habits and other activities."[519]

Furthermore, federal Canadian politicians regarded the technology as capable of inappropriately degrading access to content or communications; DPI was a discriminatory technology.[520] For American regulators, DPI rose to become an existential threat to the FCC's ability to regulate ISPs, and politicians who paid attention to the technology saw it as potentially inappropriately collecting individuals' information. In one Senate committee, a Senator asked if the surveillance of data flows for advertising

---

[515] Interview with Canadian regulator, February 1, 2012.
[516] Interview with Canadian regulator, February 1, 2012.
[517] Interview with Canadian regulator, February 1, 2012.
[518] Jennifer Stoddart, "Commissioner's introduction to DPI research volume," *Office of the Privacy Commissioner of Canada*, April 2009.
[519] Office of the Privacy Commissioner of Canada, "What is DPI?", *Office of the Privacy Commissioner of Canada*, April 2009.
[520] Peter Nowak, "NDP to introduce 'net neutrality' private member's bill," *CBC News*, May 27, 2008, accessed April 7, 2011, http://www.cbc.ca/news/technology/story/2008/05/27/net-neutrality-ndp.html.

was "just wiretapping?"[521] In a related vein, Congressman Markey asked whether such applications of the technology raised privacy concerns or interception issues. While the executive branch of the US government has not spoken directly about DPI, per se, it has routinely regarded the NSA's surveillance operations as important to national security and combating threats against the United States. In this space, the technology is regarded as a tool in a larger toolbox, as opposed to *the* tool that is responsible for defending the homeland.

In turning to UK regulators, it is apparent that they have attended predominantly to the traffic management and privacy issues associated with DPI-based practices. Ofcom's consultation in 2010 recognized that while "traffic management potentially offers some benefits to consumers there are also concerns that firms could use traffic management anti-competitively"[522] In terms of advertising uses, the Home Office, in particular, demonstrated a willingness to learn from industry when it asked Phorm "what it thinks of the advice [the Home Office] is drawing up in relation to behavioural advertising."[523] The potentially positive position of DPI has significantly shifted since the technology was introduced on the UK agenda, with one regulator stating that "[i]t's always going to come down to the purpose of the technology. I mean, DPI itself is not necessarily illegal or never to be used under any particular circumstances, so something about that purpose and what particular safeguards are in place to make sure that data is only used for that individual purposes, whether it be traffic management or investigating communications content."[524] This same regulator recognized that "there are different definitions of DPI and what is the packet, and how deep do you have to go for packet inspection. That's the big debate that goes one."[525] One of the purposes, in the UK, at least, involves using DPI for national security and foreign intelligence purposes, though it remains to be seen whether the UK government will defend uses of DPI that are

---

[521] Nate Anderson, "NebuAd CEO defends web tracking, tells Congress it's legal," *Ars Technica*, July 9, 2008, accessed March 2, 2013, http://arstechnica.com/tech-policy/2008/07/nebuad-ceo-defends-web-tracking-tells-congress-its-legal/.
[522] Ofcom, "Traffic Management and 'net neutrality': A Discussion Document, *Ofcom*, June 24, 2012, accessed November 18, 2012, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf.
[523] Darren Waters, "Home Office 'colluded with Phorm'," *BBC News*, April 28, 2009, accessed May 10, 2013, http://news.bbc.co.uk/2/hi/technology/8021661.stm.
[524] Interview with UK regulator, September 19, 2012.
[525] Interview with UK regulator, September 19, 2012.

associated with its surveillance of transatlantic communications. On the whole, then, DPI is variously defined within government circles as a beneficial tool, as a way for ISPs to potentially monetize their subscribers' traffic, as a way to derive personal insight about subscribers, as implicated in wiretapping, and 'really' about very different things depending on just how deep the inspection of packets goes. Again, regulators and members of government have focused on the implications of control related to the technology and have examined and overseen debates concerning the legitimacy or correctness of using this control to achieve a widespread set of business and 'public interest' goals. No institution has focused purely, and publicly, on the general appropriateness of embedding such control systems within telecommunications networks.

The preceding descriptions clearly show the various perceptions that different communities have of DPI, perceptions that often reflect existing interests, worries, or biases. All parties' DPI discussions contained notions of control, but communities differ on the extent of control and influence that ISPs should be able to exercise over data traffic and on the implications for such control. Throughout the cases, the various communities and government institutions have tended to focus on the specific *practices and capabilities* that are linked to the technology; such a focus often led to disputes concerning the depth at which packets were inspected and the measure of control afforded by specific deployments of the technology. Contestations over actual or supposed capacities to control communications often resulted in policy communities disputing the specific instantiations of the technologies in ISPs' infrastructures; DPI's perceived fungibility meant that communities and actors, often with significantly different technology or policy experience, talked past one another in formal and informal debate arenas. So, where ISPs and their vendor partners would sometimes provide a technical depiction of the appliances' capabilities, other policy communities would apply their own understanding(s) of the technology's technical capabilities when they made claims about the potential externalities linked with the equipment. Significantly, ISPs would often reveal as little as possible about the specific capabilities of their equipment, thus often forcing competing actors and communities to imagine 'worst case' DPI-related practices in their public contestations of DPI. The divergent positions in policy networks were often based on how parties thought networks 'ought' to function. ISPs sought to

retain economic and technical control over their networks, whereas opposing policy communities sought to advance *their own* community interests by restricting ISPs from enhancing management of packets at the core of the network, at the expense of management capacity held by the edges.

Disputes around DPI essentially fell to disagreements on the extent to which ISPs or endpoints should be primarily responsible for establishing, managing, and maintaining communications. The role of the ISP – as a minimally involved transporter of packets or deeply attentive manager of packet flows – routinely formed the backdrop of policy disputes. While policy conflicts tended to focus on the nature of specific actions, the failure to assess and agree upon or come to terms with the key issue of appropriate dimensions of network control means that DPI functions as an open symbol for issues related to privacy, security, speech, freedom, and association. It may, in fact, be *impossible* to 'close' DPI as a symbol of these broader issues because policy communities' existing interests and positions necessarily establish conflicts over where the power to control or manage packet flows should rest. At best, communities might arrive at temporary truces, where specific issues related to specific applications of DPI are settled, but ISPs that aim to 'control' subscribers' communications may permanently run afoul of free speech and privacy advocates. Similarly, ISPs may be routinely opposed by businesses whose interests benefit from ISPs being restricted in how they can interdict data flows. Given the relationship between ISPs, advocates, and some businesses, fully closing or stabilizing the contests of control might be an existential issue for communities because some in the policy network might hold positions that are entirely at odds with how other members of the network understand who should primarily control the management of packet flows. Moreover, the willingness of 'strange bedfellows' to work together makes the breadth of issues linked to DPI unusual: corporations often seen as hostile to privacy interests such as Facebook work alongside privacy advocates, consumer advocates work in tandem with advertisers, and ISPs that compete with one another support one another against potential network neutrality regulations. Tacit and short-term agreements have been, and are, reached between these often hostile policy actors, largely based on where members of these communities believe network control should rest, and over who should be able to exercise such controls. The failure to clarify

the dimensions of control, outside of when speaking about incredibly specific practices, has allowed these groups to work beside one another without necessarily giving up or compromising on key principles or positions. It is enough for parties that specific practices are moderated or rejected; the value of such successes changes depending on how specific community members would be (dis)advantaged by restrictions over ISPs' exercise of control on their networks.

Ultimately, the state of affairs concerning DPI means that it is unlikely that the politics linked to DPI are anything more than temporarily stabilized; the core issues that have been drawn out during the debates around the technology will almost certainly return to regulatory and political agendas in the future. Further, if ISPs can convince other policy communities to walk away from their existing coalitions, the argumentative strengths of consumer and civil society advocates may be diminished. Such splits will likely be based on ensuring that ISPs' or governments' interests are perceived as aligned with those of (former) coalition members. For example, ISPs might adopt fine-grained analysis of copyright infringing material in order to sway content makers and distributors away from civil society parties, so long as such agreements do not confer liabilities onto ISPs. Further, ISPs could partner with existing Web-based advertisers to sell even more highly targeted ads to Internet subscribers, or ISPs could aggressively try to recruit commerce-minded civil advocacy groups with promises that DPI would only ever be used to enhance consumer privacy, security, and choice. In effect, while the issues discussed in the previous chapters are temporarily settled and have presently defined policy networks and communities surrounding them, the current positions could change if ISPs successfully change the incentive structures around the various issues. DPI could return to the agendas with a vengeance if ISPs decide that it is in their best interests to revisit past decisions, positions, and approaches to business.

How DPI Has Been Shaped by Domestic Institutions

DPI-enabled routers and accompanying software have set the stage for debates about the degrees of control that ISPs should have over their subscribers' communications and the extent to which states should be permitted to inspect their residents' communications. While in Chapter Three I suggested that international standards bodies might be influential, this was not proven to be the case. Ultimately, the case studies demonstrated

that the technology and its potential have been framed by domestic policy contestations; such contestations have principally determined how DPI is used in Canada, the US, and UK. Contestations have often seen strange bedfellows working together, typically trying to mutually repudiate or authorize conceptions of network control that serve the bedfellows' own interests. In essence, sporadic advocacy coalitions, which have been characterized by actors sharing common positions on where control over network traffic should rest and who were mutually interested in shaping policy outcomes, have developed around the various issues and practices that were debated. The policy contestations that these coalitions formed around have transpired across a series of institutional arenas. The following table summarizes the involvement of regulatory institutions, elected political arenas, or the courts in each case, across issues.

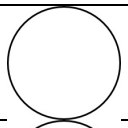
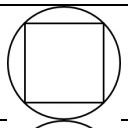
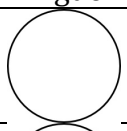
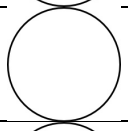
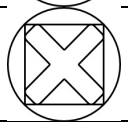
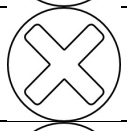
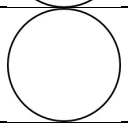
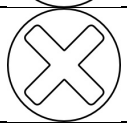
Issue	Canada	United States	United Kingdom	Outcomes
Network Management				Significantly common results
Content Control				Common regulatory results, different politicial results
Advertising				Common results through radically different processes
National Security				Similar tactics with unclear results
 = Regulatory Institution;  = Elected Political Arena;  = Courts				

Figure 6: Government Institutions Involved in Adjudicating DPI-Based Practices

In terms of policy arenas, each case reveals unique characteristics. The Canadian case shows that regulatory institutions were principally where private uses of DPI were adjudicated. The United States, in contrast, saw its regulator overturned in the issues it took up; elected political arenas and courts have been the spaces where debates have been settled. Finally, the UK revealed a mix of regulatory and elected political arenas as where debates were settled; in this case, weak governmental institutions sometimes had their decisions rebuffed in the face of political resistance. Despite variations in the institutions that took up issues, there were remarkably common *results* from the respective countries' policy debates. Though it might, at first glance, seem that significantly different

conclusions would be reached based on the particularities of courts, past regulatory decisions, and even political interests, this has not been the case. In fact, the only instance where political arenas led to significantly *different* conclusions was around copyright management; similar agreements were ultimately reached concerning content control (i.e. management of applications and protocols).

In both the American and British cases, we saw how a series of government institutions were, or became, intractably interlinked as a result of policy advocacy by policy entrepreneurs; as a result, attempts to understand purely how institutions will address an issue demand a broader conception of the political arrangements within which the issues are situated. Games and compromises related to the interdiction of data flows by ISPs, as a result, must be considered across the breadth of actual and prospective domestic (and, in the UK, European) policy arenas: 'winning' in one arena is no guarantee of actual success in how any issue is ultimately framed. Entrepreneurs have routinely 'forum shopped' when choosing regulators, political officials, or other government institutions to try and resolve problems according to the entrepreneurs' interests. The impetus for such shopping is predicated on whether other arenas are perceived as receptive to a policy community's attempt to frame an issue. Corporations and members of civil society alike have often turned to a series of (perceived) friendly forums to authorize or condemn the practice in question. Corporate success in advocating its positions across all forums tends to be linked to whether the practice in question is associated with pre-existing business operations and can be exempted from existing wiretapping, privacy, or data protection laws. Other policy communities have enjoyed success when novel practices are (prospectively) introduced or when ISPs' actions demonstrate significant externalities. Such novel practices, even when they *may* be legal or *may* be privacy protective have been found deficient: such findings speak to the range of potential ways to 'attack' an issue on the grounds of ethics, law, and politics. The policy communities opposed to various data interception and modification practices have availed themselves to all of these avenues of attack, revealing that unless a company can defend its practices on all these grounds, the potential exists for policy entrepreneurs to successfully contest a given practice.

Based on the findings and excluding state-specific surveillance, it appears that the Canadian telecommunications and privacy policy networks have generally been left alone by elected legislative officials, insofar so such officials have not been significantly involved in how communications are monitored and mediated by corporate parties. This position is solidified based on the shock that arises whenever the federal government interferes with the CRTC's decisions; attempts by federal politicians to overturn or contest decisions reached by independent regulators are regarded as untoward and unusual by members of the Canadian telecommunications policy network. The American situation suggests that interfering with communications is ultimately not a *regulatory* issue so much as a political and legal issue. In the US, regulators are largely limited in their capacities so long as companies are not violating contractual guarantees, though the elected political arena is not necessarily able to legislate for change. Instead, this arena is presently best suited to negotiating truces or agreements between or across policy communities. The American legal arena is where issues can actually be addressed. Finally, the UK shows a combination of regulatory and political involvement with the interception of communications, but with the twist of the European Union 'teaching' the UK government what constitutes inappropriate means of accessing and modifying data in transit. Unlike non-European states, the UK is unique insofar as even after regulatory or political decisions are made, extra levels of appeal exist. Regardless, despite the differences in *processes* to regulate the interception of communications themselves, the *outcomes* of issues have ultimately been similar. These similarities speak to the willingness of policy entrepreneurs, in each jurisdiction, to advance common causes in their respective countries and to their success in finding receptive (and suitably influential) arenas to hear their side of the issue.

Despite politicians having been involved in the US and UK cases, it isn't clear that the interception of communications fits within any one political party's orientation. In terms of domestic interception, political parties have not taken uniform positions on the issue. Instead there have been specific members of government that have taken interest in such interceptions and subsequently raised it to the attention of their colleagues, often only after having been alerted to the issue by either the media or civil campaigners.

Issues have been characterized and contested by a typically Internet-savvy group of actors. They have, principally, disagreed over the appropriate dimensions of control that ISPs should possess over communications infrastructure. Despite the significance of the Internet architecture for business, generally, only firms like Google, Yahoo!, Facebook, Microsoft, and other businesses that are heavily dependent on the Internet for revenues tended to take part in political and regulatory debates. Generally absent from the debates were established journalistic bodies, save for the BBC's and CBC's prominent roles in their respective states' regulatory proceedings. Such (un)involvement is significant, insofar as despite the *prospect* of ISPs affecting newspaper and journalistic business practices, only state broadcasters were significantly involved in the political and regulatory proceedings. In both cases, these broadcasters were involved in next-generation content dissemination strategies, suggesting that their involvement was tied to direct interest or stakes in the proceedings' outcomes; the sole fact that they were public companies was not necessarily sufficient for them to involve themselves in the issues.

In terms of state surveillance, each case reveals how legislative and executive political domains have been the key arenas within which the issues have arisen, though secretive US surveillance is presently being challenged in American courts. All cases reveal governments advancing public legislation though the need for such legislation as a precursor to the surveillance remains unclear. The American intelligence agencies and executive branch of the government have adopted tortured understandings of law to justify surveillance behaviours and have relied on the legislative branch only to legalize already-ongoing practices. It appears that, given recent revelations that British intelligence has been massively monitoring data flows, repeatedly rebuffed UK legislation may also be predominantly meant to legalize surveillance that is already ongoing. It is possible that Canada, as one of the 'Five-Eyes'[526] might be trying to pass its own legislation for similar purposes, though evidence to support this claim is presently circumstantial at best. In all cases, including that in Canada, civil liberties campaigners have sought to raise government surveillance issues to the attention of the media and public in order to develop opposition to the authorizing legislation. The ultimate efficacy

[526] The 'Five-Eyes' include Canada, the United Stated, United Kingdom, Australia, and New Zealand. The countries have a collaborative intelligence collection and sharing regime, where they agree to more freely share information with one another than with other 'non-eyes' countries.

of such opposition, however, has been called into question as more information is disclosed concerning intelligence services' surveillance operations. Successes in stopping the public legalization of government surveillance for national security purposes do not seem to have clearly translated into stopping the *practices* of government surveillance for national security purposes.

Conclusion

In aggregate, what conclusions can be drawn from how institutions and policy communities have taken up the surveillance of communications traversing corporate-owned telecommunications networks? First, it is apparent that while each state possesses its own mechanisms to take up such surveillance practices, the mechanisms often result in common outcomes. Significantly, these outcomes all reveal that *practice* creep has taken place. Based on existing normative understandings and regulatory positions, suggestions that the entirety of packets could be analyzed might have been rebuffed at the inception of the public Internet, but today, the question is what *degree* of surveillance is appropriate on telecommunications networks. The nature of the debates today does not so much show regulators and policy communities as more willing to adopt nuanced views of telecommunications networks as it does an acceptance of a fine-grained awareness of daily activities that are linked to corporate behaviours. The practices that are linked with such surveillance and control, rather than the very act of the surveillance or attempts to control data flows, have become the debates of the day. Fighting against the specific routers and accompanying software code that enable such behaviours in the first place are regarded as fools-campaigns.

Second, it is clear that Internet issues see a range of 'traditional' arenas acting as the sites of conflict between very traditional telecommunications companies and (typically) much younger opposing policy actors and communities. Though some long-term policy actors have been involved in the various policy debates (e.g. Public Interest Advocacy Centre, CBC, and BBC), companies and organizations that emerged with the Internet have driven the majority of the conflicts. As a result, even when policy actors have radically different outlooks on something like privacy, those actors can come together to oppose an ISP's attempts to enhance its control of telecommunications systems. While Google and Facebook and the EFF might partner against the ISPs, they

are all involved in conflicts with one another outside of telecommunications regulatory processes. The transport mechanism for communication is regarded as something that many of the 'young' actors must defend and, after doing so, they can return to their routine conflicts against one another.

Third, in examining national security it appears that 'successes' in preventing overly invasive government surveillance may be illusory. Despite the public importance of repudiating legislation or legally opposing invasive intelligence gathering it is unclear whether such public successes have translated into the actual cessation of undesired practices and actions. The current 'solution' seems to be to rely on whistleblowers to reveal government deceptions, but the efficacy of such a solution remains dubious. Efforts to prevent and criminalize leaks have increased and will continue to do so. Even when whistleblowers do come forward, the government does not necessarily cease its surveillance practices. What is evident is that, even in the face of whistleblowers, it can take years of court action to secure a legal cessation of government practices. The 'simple' revelation of the actions themselves does not appear to lead a legislatively significant *political* outcry, which limits any hope of a speedy cessation of surveillance practices after once they have been discovered. Even if such a political outcry was to occur, its effectiveness would be dubious. Given the willingness of the executive branches of government and intelligence services' to stretch or torture the meaning of legislation, even efforts to legislatively rein in national security practices may fail.

The contests surrounding DPI have shown elite policy actors competing with other elite actors, in specialized political and high-expertise regulatory arenas, over who should control the dissemination of information on the Internet, and to what extent such control should be permitted. These contests have created strange bedfellows. These contests expose policy entrepreneurs who forum shop until they find a friendly forum to 'solve' the relevant problem in the entrepreneur's favour. They reveal a divide between pre- and –post-Internet actors. Finally, they show the cacophony of parties that *can* become concerned about ISP-driven surveillance when it is clear that such surveillance runs against the parties' own interests.

In turning to the final chapter I take up the concepts of surveillance and privacy that have pervaded the dissertation. Specifically, while these concepts are necessary to

understand the issues related to DPI in a policy context, they are insufficient to understand the magnitude of what it means for citizens' communications to be massively monitored, mined, and modified by network controllers. Given the potential to affect or monitor communications using DPI it is important to understand the technology within the context of relevant democratic theory: What does it mean for liberal, democratic, Western states when mass surveillance appliances are inserted throughout communications networks? What can be done to avert the worst consequences of such surveillance and ensure that the Internet can be used to facilitate, instead of undermine, the democratic potentials of the state?

Chapter 8: Managing the Threat to Deliberative Democracy

In the previous chapter, it became apparent that even though policy actors contested what Deep Packet Inspection (DPI) *meant*, they all generally positioned themselves and the issues in terms of control: who should control the flow of data packets, and why, and under what conditions? Such discussions of control were often either implicitly or explicitly linked to arguments about the permissibility of monitoring packets, and whether such monitoring constituted a justified kind of surveillance or an appropriate infringement on individuals' privacy. While various actors and policy communities were sensitive to the surveillance- and privacy-characteristics linked to DPI, they rarely considered DPI within a broader political context. As a result, the policy arenas and actors focused on specific comparative policy issues instead of on how DPI might affect citizens' abilities to engage in political deliberation that is meant to guide and legitimate state actions. This chapter places DPI within the broader context of normative deliberative democratic theory, and suggests that the technology and its associated practices are perhaps most appropriately critiqued and understood against the backdrop of how DPI could affect political discourse in democratic states.

This final chapter concludes the dissertation by discussing why the concepts of surveillance and privacy are helpful, but ultimately insufficient, to appreciate the democratic significance of deep packet inspection equipment. In response, I suggest that deliberative democratic theory can provide useful normative critiques of DPI-based packet inspection. Moreover, these critiques can result in practical policy proposals that can defray DPI-based practices capable of detrimentally stunting discourse between citizens using the Internet for communications. The chapter concludes with a discussion of how this research can be advanced in the future; while I have sought to clear away some of the murk concerning the technology, my research represents only the first of many steps to reorient Internet policies such that they support, as opposed to threaten, democratic values.

DPI as a Surveillance Technology

Since deep packet inspection devices involve monitoring traffic and influencing users' behaviour, they are best framed as surveillance equipment. DPI provides network

operators with heightened capacities to survey data flows at network-wide as well as user-specific levels. Deep packet inspection, consequently, is not *just* a surveillance technology, but is one that infringes on individual's privacy based on how DPI can interact with individuals' personal information. As will become evident, the concepts of surveillance and privacy are arguably unsuitable to comprehensively respond to the implications of DPI-related practices. A democratic turn is needed to orient the discussion and solutions to such practices.

Surveillance has always focused on reacting to identified criminal and other deviant behaviour, and today it is often massive in scale and routinely directed towards pre-emptive social control. Contemporary surveillance practices entail "the focused, systematic and routine attention to personal details for purposes of influence, management, protection, or detection" and are dependent on regularized or predetermined "protocols and techniques."[527] The aim of monitoring persons is to act on the individual vis-à-vis mediating the practices of the entire community.[528] So, while information is derived from individuals or their actions, such information is mobilized and made actionable only after understanding individuals within their broader relational structure. The degree of awareness enabled by DPI equipment can vary depending on how and why information is mobilized: it can reveal 'bad' customers on ISP networks who are using protocols claimed to generate significant network congestion; it can identify and restrict the ability to use applications that threaten ISPs' own product offerings; and it can be used to modify data and unmask the individuals using 'abnormal' encryption and anonymization techniques. Such practices demonstrate the *productive* nature of surveillance, insofar as the practices are aimed at generating some kind of benefit(s) for the network controllers.

Recent contributions to surveillance literatures take pains to recognize that surveillance studies ought to study the 'assemblage', or the groups, parties, technologies, practices, and discourses that, in aggregate, constitute the 'new surveillance'. Scholars such as Haggerty and Ericson suggest that surveillance technologies "do not monitor

---

[527] David Lyon, *Surveillance Studies: An Overview* (Cambridge, UK: Polity, 2007), 14.
[528] Kevin D. Haggerty and Richard V. Ericson, "The New Politics of Surveillance and Visibility," in *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson (Toronto: University of Toronto Press, 2007), 3.

people *qua* individuals, but instead operate through processes of disassembling and reassembling. People are broken down into a series of discrete informational flows which are stabilized and captured according to pre-established classificatory criteria."[529] The informational flows that are collected can include 'content' and metadata alike, and, in the digital context, DPI affords network controllers the ability to perceive, capture, and process considerable amounts of metadata. Information that previously would have been too 'fine' to be caught in network controllers' surveillance sieves or too voluminous to process can now be captured and analyzed. Moreover, software updates mean that the potentialities of specific DPI appliances are limited only by the existing hardware and applicable vendor capabilities; updates let surveillance processes, targets, and objectives shift without necessarily mandating the purchase of new equipment.

Given the multitude of actors interested in using DPI and the diversity of their goals, the very fungibility of DPI means that no particular, single group or institution can be seen as guiding surveillance practices.[530] As such, we cannot examine any particular organization but instead must cast our attention to the complexity of surveillance practices, behaviours, and actors to make sense of how data flows are analyzed and processed. In only some cases could ISPs' actions be considered systematically using "personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[531] Specifically, where ISPs use DPI as a kind of 'digital sieve' to treat all specified kinds of traffic as 'second class' data traffic, there isn't a necessary systematic use of personal data. In contrast, where DPI is used to develop predictive ascriptions of consumer identities, personal data is clearly used as part of a mass data surveillance and processing practice. However, the use of personal

---

[529] Kevin D. Haggerty and Richard V. Ericson, "The New Politics of Surveillance and Visibility," in *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson (Toronto: University of Toronto Press, 2007), 2.

[530] The relative fungibility of technology, while a characteristic of DPI, is not *solely* a characteristic of DPI. Other technologies, such as contemporary pharmaceuticals, see actors with diverse interests guiding policies and procedures around the dispensation of medications. As examples, manufacturers may be motivated by profit to generate new drugs, whereas regulators may be concerned about the *safety* of those medicines, whereas consumer advocates may be concerned about patent durations linked to medicines and the production of generics, and so forth.

[531] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms," *Roger Clarke's Web-Site*, last updated August 7, 2006, accessed August 9, 2013, http://www.rogerclarke.com/DV/Intro.html.

information shapes the significance of the practice and reveals how the contours of DPI's potentials can be highly variable.

Beyond a discussion of surveillance of the specific individual or of the population is a question of breadth. How much of an individual's generalized characteristics are paid attention to, and what is and is not watched for? While mass surveillance may accidentally capture information beyond that sought, targeted surveillance - the specific focusing-on-an-information type - may provide the surveying party with a deep field of data that is relatively limited in scope. In terms of DPI, where targeted surveillance might be the equivalent of calibrating the surveillance sieve to monitor for highly specific protocols or content, mass surveillance might entail a broader attempt to 'understand' network traffic and include out-of-line analysis of the data traffic to ascertain new encryption or anonymization techniques, or to better identify and act on previously-unknown data protocols. Regardless of the 'kind' of surveillance, be it mass or targeted, the associated practice(s) is "invasive because, independent of whether data protection principles have been respected, the individual's social actions are removed from the intersubjectivity that ground the identity and enables him or her to enter into social relationships with others."[532] Surveillance, in essence, strips individuals from their particularities in accordance with the norms and principles guiding the practices, to the effect of embedding the individuals and their communities within those practices. Moreover, the practices associated with DPI-driven surveillance predominantly empower network controllers, with network *subscribers* possessing limited knowledge of, or agency over, how these practices are developed, deployed, and updated over time. As such, network controllers' actions are embedded in a highly asymmetrical relationship. Short of raising specific actions to regulatory or political agendas, subscribers are effectively unable to restrict controllers' surveillance without deploying highly technical countermeasures.

However, given that DPI is involved in surveillance actions, it might be expected that the power dynamics invoked in the regime of privacy protection could correct the balance. Privacy might offer a way to rebalance the power asymmetries between the

---

[532] Valerie Steeves, "Reclaiming the Social Value of Privacy," in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock (Toronto: Oxford University Press), 206.

watchers and the watched. Unfortunately, neither focusing on places or persons offers particularly compelling means of restricting DPI-related practices. In the case of the former, privacy expectations have often been linked with the domains in which an actor behaves. As a result, expectations of privacy may be heightened in the home and diminished in public spaces. The protection of 'places not people' is problematic in the case of DPI-driven surveillance because it leaves unclear the privacy expectations of browsing the public Internet (outside the home) from within a person's private domicile.[533] Moreover, various legal regimes have evolved such that persons experience reductions in their expectations of privacy after either abandoning something (e.g. trash at the curb) or communicating something to a third-party. Within the context of telecommunications, there are pieces of information that individuals *must* give up as a precondition of Internet access: they must reveal routing and address information to their direct network controller and to all others involved in transiting traffic to its destination(s), and they must reveal this information in a manner through which another party could subsequently derive meaning from the data. The 'traditional' protection of communication based on spatiality that often establish 'reasonable' expectations of privacy, then, does not effectively apply where the Internet - and its attached sensor systems - are predicated on revealing prospectively personal information to communicate in the first place.

Efforts to focus on the "nature of the knowledge discovered" to ascertain whether monitoring a communications flow is privacy invasive are similarly problematic. While such an approach "might add to our understanding of privacy in a way that allows us to further explain the bad taste that data mining leaves in so many of our mouths,"[534] it does not correct or alter the 'Russian doll' syndrome that is often associated with privacy. Specifically, when focusing on the nature of discovered knowledge, attention is given to whether the information relates to 'core' or to 'extraneous' information about a given person. Distinguishing between core and non-core data to gauge the nature of discovered

---

[533] Anne Utech, "Ubiquitous Computing and Spatial Privacy," in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock (Toronto: Oxford University Press), 100.

[534] Jason Millar, "Core Privacy: A Problem for Predictive Data Mining," in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock (Toronto: Oxford University Press), 111.

knowledge presumes that the individual must be the core site of analysis to detect problematic practices. At issue is that what is 'extraneous' to a specific individual could be 'core' to a community that the individual is (or has been) associated with. So, in cases where DPI analysis doesn't identify an *individual* specifically, but instead ascertains characteristics of a person's community (e.g. particular application users, subscribers using particular amounts of bandwidth or services), the act of so monitoring may not 'violate' individuals' personal dignities, but such guarantees don't necessarily wash the 'bad taste' out of people's mouths.

Both of the aforementioned means of ascertaining privacy harms - based on place or information derived about an individual - are deeply grounded in liberal conceptions of privacy that recognize privacy as preserving "negative space around individuals who are already fully formed or mostly fully formed, affording shelter from the pressures of societal and technological change."[535] Most liberal understandings of privacy only register 'problems' when individuals experience or are subjected to an evident harm. Governments and corporations often 'address' issues linked to surveillance actions by requiring individuals to consent to the relevant practice, though few individuals necessarily understand precisely what they are consenting to, or even that they consented in the first place.[536] And even when consent has been received in the context of DPI-related practices the automated sieving of data packets to slow down or discard 'problematic application' packets may not constitute a privacy (as opposed to a market) issue so long as the subscriber's name isn't permanently attached to the sieving practice. There are productive responses to these liberal understandings of privacy. Kerr suggests that online service providers, such as ISPs, should be recognized within a liberal contractual regime as possessing fiduciary obligations of loyalty to their subscribers:

> "…the duty of loyalty forbids the trusted party from furthering its own self-interest where doing so would be detrimental to the best interests of the trusting

[535] Julie Cohen, "What Privacy Is For," *Harvard Law Review* 126: 1904 (2013), 1907.
[536] Mark A. Graber, Donna M. D'Alessandro, and Jill Johnson-West, "Reading Level of Privacy Policies on Internet Health Websites," *Journal of Family Practice* 51(7): 642 (2002); Irene Pollach, "What's Wrong with Online Privacy Policies?" *Communications of the ACM* 50(9): 103 (2007); Joseph Turow, "Americans and Online Privacy: The System is Broken (research report)," *The Annenberg Public Policy Center of the University of Pennsylvania*, June 2003, accessed September 7, 2013, http://www.ftc.gov/bcp/workshops/infoflows/comments/030618turow.pdf.

> party. If a conflict of interest arises, the duty of loyalty demands the trusted party to remain faithful to the trusting party, despite its own reluctance to do so."[537]

For Kerr's formulation to take action in the case of DPI, subscriber privacy interests would need to be articulated in a manner that the ISP could subsequently act on. Significantly, his approach does shift the onus on ISPs to 'take care' of the subscriber. While the Canadian situation may provide some guidance, based on the federal Privacy Commissioner's approval of DPI for some uses so long as subscribers are meaningfully informed of the relevant practices, it remains unclear that either of these two approaches necessarily remedy the problem of focusing predominantly on *individuals* instead of individuals *and* communities. The 'party' referred to in most contracts is a specific individual or organization: ISPs do not sign contracts with their entire community of users. So, the breadth of these two responses may be unduly limited.

More 'socialized' conceptions of privacy have been put forth by a raft of contemporary scholars. For some, recognizing privacy as critical for individual *and* community goods means that privacy might be less likely to 'lose' when juxtaposed against competing community goods (e.g. community privacy versus community security) as opposed to when community goods 'trump' individual interests (e.g. individual privacy versus community security interests).[538] Moreover, by posing privacy as a social value the concept might be realigned in legal frameworks; the conceptual shift recognizes privacy as being "in society's interests. Individual liberties should be justified *in terms of their social contribution.* […] The value of privacy does not emerge from each form of privacy itself but in the range of activities it protects."[539] The emphasis on privacy's social contribution, in the domain of the political, lets privacy be seen as "a meta-concept that may support increasingly sophisticated and layered interpretations of other concepts that inform Charter values. […] If dignity is concerned with the promotion or safeguarding of the conditions necessary for the realization of full personhood, privacy

---

[537] Ian Kerr, "Online Service Providers, Fidelity, and the Duty of Loyalty," in *Ethics and Electronic Information*, edited by Thomas Mendina and Barbara Rockenbach (Jefferson, North Carolina: McFarland Press, 2002).
[538] Priscilla Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (Chapel Hill: University of North Carolina Press).
[539] Daniel Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, 2008), 173–5. Emphasis added.

is the tool that may, in some instances, help to accomplish this end."[540] Such attempts to recognize the community's value extend beyond acting as 'just' a political game. By providing an account of privacy's value, as situated in the community and thus based on intersubjective grounds, we can make the step that "[s]elfhood and social shaping are not mutually exclusive. Subjectivity, and hence selfhood, exists in the space between the experience of autonomous selfhood and the reality of social shaping. It is real in the only way that counts: we experience ourselves as having identities that are more or less fixed. But it is also malleable and emergent and embodies, if we are honest, that too accords with experience."[541] A 'holistic' accounting of privacy constitutes a more real accounting of the world we live in and, thus, can promote a healthier legal and political system based on the nature of human experience itself.

So, what does this 'socialized' conception of privacy mean within the context of DPI-driven surveillance? First, it lets us acknowledge that an individual may or *may not* need to be specifically aware of an infringement for a normative violation to have occurred. The 'sieving' of communications data flows inherently demands examining the payload of a packet - that holding the content of the communication - and efforts to examine this information may be regarded as prying into something that, despite having little *material* value, entails infringing the privacy of the intersubjective relationship(s) between the parties involved in the communication. Moreover, though no permanent link between personally identifying information and DPI practices may occur, individuals may stifle actions because they fear such linkages could be made to the detriment of communities they are linked with. Here, despite harm not necessarily befalling an individual, the potential 'chilling' effects that surveillance could have on a community could be used to register a privacy infringement.

DPI-based surveillance practices raise privacy concerns, but, more significantly, these practices raise existential concerns over the potential to speak freely in a democratic state. Given that DPI technologies can broadly act on communications, democratic theory can be used to recognize the potential implications of mass surveillance practices while

---

[540] Daphne Gilbert, "Privacy's Second Home: Building a New Home for Privacy Under Section 15 of the Charter," in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock (Toronto: Oxford University Press), 149–50.
[541] Julie Cohen, "What Privacy Is For," *Harvard Law Review* 126: 1904 (2013), 1909.

also modifying the ethical conditions that such surveillance practices are implicated. Within the scope of democratic organization, at least three democratic models present themselves: liberalism, republicanism, and dialogical. Per the liberal view, the state's role is to guarantee individual rights and enable voting blocs through which citizens enact change. In contrast, the republican position sees institutions as mechanisms through which citizens express their political will, though it assumes that there are (or can be) common or unified political ethics. Consequently, a politically diverse society that pursues irreconcilable political ends can lead to a tyranny of the majority.[542] In contrast to these two models, a dialogical approach to democratic theory, such as that exhibited in deliberative democratic theory, recognizes the situatedness of individuals *and* their communities simultaneously, with dialogue cutting across both individual and macro (i.e. community-based) subjectivities. The result is that dialogue fosters the conditions of the individual and the state, without giving priority to either. However, this emphasis on dialogue and discourse also means that stymying the capacity to communicate undermines the redistributive potential of democratic politics that are sensitive to non-majority positions and voices. Given the pluralism in contemporary political environments, and the need to generate consensus across communities for democratic decisions to be regarded as legitimate by a population, and the contemporary mass-adoption of the Internet as a key medium of communications, deliberative democratic theory offers a useful theoretical lens to analyze contemporary communications surveillance because of its focus on the need for free communications by individuals, across communities, in often diverse political climates. Effectively, the processes of acting on the routine communications of citizens, the conditioning of the means by which the sharedness of experience is possible, and the commercialization or capturing of data for government surveillance, places at risk the very capacity to engage in deliberative democratic communications. It is essential to preserve and enhance such communications if contemporary pluralistic states are to effectively legitimize their political decisions, and especially those decisions that can affect a range of often disadvantaged or underprivileged members of society.

---

[542] Jürgen Habermas, "Three Normative Models of Democracy," in *The Inclusion of the Other: Studies in Political Theory,* ed. Ciaran Cronin and Pablo De Greill (Cambridge, Mass.: The MIT Press, 1998).

Deliberative Democracy Threatened

Deliberative democratic models are characterized by their emphasis on free speech as the essential character of democratic governance. These models of politics stand in contrast to more liberal- and communitarian-oriented models of democracy. These latter models "posit a unitary subject, whether the isolated ego or the undifferentiated communal subject," whereas deliberative approaches take seriously "the multiple differences between subjects within pluralist societies…dialogue and difference are central to the deliberative model."[543] In taking seriously the pluralist character of human subjectivity, individuals are ethically obligated to consider attitudes and practices that are associated with their own *as well as* their community's best interests;[544] arriving at just policy decisions, then, entails coming to positions after engaging in deliberation. Deliberation is aimed towards producing "reasonable, well-informed opinions in which participants are willing to revise preferences in light of discussion, new information, and claims made by fellow participants."[545] Though consensus is not always achieved, by involving all participants in the deliberation, individuals can expand their own understandings and, so long as all parties are permitted to engage in the deliberation in a substantive manner, all actors can see themselves reflected in the outcome of the deliberations. Habermas emphasizes the importance of taking individuals and the communities they exist in seriously when asserting the 'co-originality' of both rights and popular sovereignty. As summarized by Chambers, this co-originality means that "[t]here is no People's will to speak of without rights: there are no rights without some theory of popular sovereignty to create an original justification."[546] Focusing primarily on either communities or individuals, then, masks the nature by which individuals and their communities are bound to one another.

The deliberative model can be regarded as *orienting* political practice rather than prescribing particular processes that a democracy must adopt. That is to say, the

---

[543] Lincoln Dahlberg, "The Internet and Democratic Discourse: Exploring the prospects of online deliberative forums extending the public sphere," *Information, Communications & Society* 4:4 (2001), 616.
[544] Iris Marion Young, "Activist Challenges to Deliberative Democracy," *Political Theory* 29:5 (2001), 672.
[545] Simone Chambers, "Deliberative Democratic Theory," *Annual Review of Political Science* 6 (2003), 309.
[546] Simone Chambers, "Deliberative Democratic Theory," *Annual Review of Political Science* 6 (2003), 310.

deliberative model functions as a critical and normative means by which existing democratic systems can be examined; few, if any, theorists genuinely believe that a deliberative model could be 'fully' instantiated. Ideally, 'better' instantiated deliberative democracies will see parties who are traditionally excluded from policy and political engagements not just *take part* in deliberations and decisions but able to *initiate* discussion of problems and proposals.[547] Given that deliberative democracies are predicated on communication as the means of arriving at consensus, or at least genuine engagement between involved members of the community, a series of basic conditions must be met to engage in speech and discourse that is simultaneously supportive of the individual and their community. These conditions include:

- The individual must be willing to assume the views held by other discursive partners.
- The public sphere (where individuals formally communicate with one another) cannot be distorted by undue coercion.
- A liberal environment that emphasizes individual freedom must be maintained;
- The elements of private society that would be affected by imposing a particular law must be recognized and permitted to enter the communicative discourse.[548]

It is essential that individuals be able to communicate with one another without the perception of coercion. Habermas uses the term 'coercion' expansively, and it can be taken to include non-democratically legitimated surveillance that could detrimentally affect a person's behaviour.[549] Specifically, ubiquitous surveillance has a normative implication - that individuals are not free to "make up their own minds about ideas big and small, political and trivial" - and an empirical implication - that "surveillance inclines us to the mainstream and boring … when we are watched while engaging in intellectual

---

[547] Iris Marion Young, "Activist Challenges to Deliberative Democracy," *Political Theory* 29:5 (2001), 686.
[548] Jürgen Habermas, "A Genealogical Analysis of the Cognitive Content of Morality," in *The Inclusion of the Other: Studies in Political Theory*, edited by Ciaran Cronin and Pablo De Greiff (Cambridge, Mass.: The MIT Press, 1998), 42-44.
[549] See for example: David Lyon, *Surveillance Studies: An Overview* (Cambridge, UK: Polity, 2007); Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithica, New York: Cornell University Press, 1997); Julie Cohen, "Examined Lives: Informational Privacy and the Subject as Object," 52 *Stanford Law Review* (2007).

activities, broadly defined … we are deterred from engaging in thoughts or deeds that others might find deviant. Surveillance thus menaces our society's foundational commitments to intellectual diversity and eccentric individuality."[550] In the context of the Internet, the pervasive surveillance of communications is often undertaken for commercial as well as national security purposes. In the case of commercial uses, DPI can be used to dictate what individuals are 'really' interested in and skew actions and discourse in the process. While national security purposes see DPI as one part of a multi-element analysis process, such purposes also aim to mediate data that the state regards as relevant for security practices. The result of this latter surveillance is to coercively limit the range of state residents' discourse; failure to so limit discourse could have unknown consequences in the future. As a result, residents may internalize that 'abnormal' actions must be avoided.

Commercial surveillance practices that DPI makes possible might be regarded as either benign or as not intentionally harmful towards individuals because while such practices are often embedded in market logics concerning efficiency or revenue, the primary aim of ISPs is not to *harm* subscribers with whom ISPs hope to maintain a long-term business relationship. Despite this non-intention to harm, such purposes affect "the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance."[551] Often the goal of such ISP-driven surveillance is to persuade subscribers towards certain courses of action; to use or not use particular applications, to curtail specific means of content dissemination, to purchase certain goods based on online behaviours, and so forth. While such actions are 'benign', they function by subtly influencing persons to change their actions (e.g. receive or disseminate content, or use certain applications as opposed to others, in a manner preferred by network owners) or by tracing and advertising users' actions as they cross the Internet until an individual succumbs to spending money in a moment of weakness. Moreover, when and if DPI-led surveillance practices are linked to data aggregation for mining purposes, it becomes possible to sort and discriminate against specific subscribers based on what they do online, who they do it with, and the times at which they engage in

[550] Neil M. Richards, "The Dangers of Surveillance," *Harvard Law Review* 126: 1934 (2013).
[551] Neil M. Richards, "The Dangers of Surveillance," *Harvard Law Review* 126: 1934 (2013).

actions. In aggregate, these power asymmetries derived from significant ISP awareness of subscribers' actions can either outwardly affect how a person communicates or acts online (if they know of the surveillance) or can modulate or influence behaviour in an invisible fashion (if individuals are unaware of the surveillance). Regardless, the intentional or guided shifting of *how* one communicates (e.g. text versus video, by disseminating cultural products versus receiving cultural products) affects the ability for parties to engage in deliberation with one another by (re)forming the very medium that makes digital communication possible.

Similarly, shadowy government surveillance negatively affects the ability of individuals to engage in deliberative communications. The blanket surveillance of Internet communications by government "menaces our intellectual privacy and gives the government too much power to blackmail or discriminate against the subjects of surveillance."[552] Such activities, though performed in the name of 'security' can have the opposite effect. DPI technology can be used for purposes other than those originally intended; the technologies functionally create points of vulnerability within communications networks, points that can potentially be 'taken over' by third-party actors.[553] So, not only does government surveillance have a similar direct and indirect effects on citizens as commercial surveillance, insofar as citizens may restrict their speech or moderate their actions, state deployments of DPI can have the effect of injecting vulnerabilities and weaknesses into communications networks that can be exploited by third-parties to monitor and interdict citizens' communications.

The activities of ISPs and sovereign states to 'master the Internet' have the effect of undermining the communicative and intellectual privacy that individuals and their communities experience online. Moreover, such efforts directly establish environments that are 'censorious', in the sense that persons are 'nudged' towards options, attitudes, and actions that are preferred by network owners instead of being *blocked* from reading content or deliberation with others. While some scholars of digital deliberative democracy assert that individuals' personal interests will lead them to enter 'discursive

---

[552] Neil M. Richards, "The Dangers of Surveillance," *Harvard Law Review* 126: 1934 (2013).
[553] Susan Landau, *Surveillance of Security: The Risks Posed by New Wiretapping Technologies* (Cambridge, Mass.: The MIT Press, 2010).

enclaves',[554] such scholarly deliberations have principally focused on how association and communication may develop on the Web. In the case of DPI, not just Web but all Internet communications are (re)structured by network owners, often without the relative transparency of 'choosing' to join a particular deliberative online community. The effect is that the means by which deliberation is conducted online can be shaped, refined, and modulated by way of technical decisions by network controllers, decisions that have the effect of directly or indirectly influencing the means in which individuals communicate.

The actions that network controllers undertake represent an exertion of governance over the medium of communications that often lacks democratic involvement. As was revealed in all of the case studies, though representatives of civil society (and, to an extent, a handful of individuals) took part in deliberations over how DPI ought to be governed, such deliberations were largely *in reaction to* actions already undertaken by either ISPs or government. That a highly elite policy network has been involved, often either by way of the courts, specialized parliamentary or senate hearings, or telecommunications or privacy regulatory environments, means that the general population has not - and arguably *cannot* - take up the issue of how their communications environment is being modulated. Moreover, although legislators have taken up DPI in highly restrained ways - usually as pertains to specific instantiations of the technology - there has not been a sustained discussion concerning the ramifications of restricting individuals from communicating in bandwidth-rich formats (e.g. streaming video, uploading of amateur video and commentary, etc.). Politics has not significantly taken up the fact that the conditions of deliberation themselves are being affected at the level of infrastructure. The governance of Internet infrastructure has been left in the hands of high-expertise regulators who are often focused on market-driven competition principles, which has meant that the actual governance of DPI has been taken up by non-elected political appointees and driven by the agendas of network controllers, network vendors, and select members of civil society.

Ultimately, DPI poses a threat to flourishing deliberative democratic models. This model is important for normative reasons – it logically lets us conceive of the individual and community as equally important, rather than prioritizing either aspect of the political

---

[554] Cass Sunstein, *Republic.com* (Princeton, New Jersey: Princeton University Press, 2001).

community – as well as for practical reasons – its focus on communication in particular is incredibly relevant for understanding and thinking about a world wherein digital communications dictate the capabilities of individuals, communities, corporations, and states alike. As a result, deliberative democratic models offer an ethical framework against which we can judge the contemporary mode of Internet governance while opening up potential practical responses to the most harmful of DPI's practices. DPI can, in effect, be seen as posing empirical and normative threats to realizing deliberative democratic principles. Empirically, the restraints on communication as a result of network throttles negatively affects individuals' abilities to communicate in particularly 'rich' ways: through live video, high-definition music, and other multimedia formats. To be sure, no deliberative democrat asserts that such mechanisms are *required* to engage in deliberation; talking and writing letters are both (in principle) effective ways of conducting discourse. But, with successive generations that have grown up with richer means of communicating, and with contemporary generations that are often as (or more) comfortable processing a complicated video montage as they are writing an email, it is essential that the *contemporary* medium of communication enjoy a degree of respite from surveillance such that individuals *can* communicate using the medium of their day.

The empirical nature of DPI-driven throttling, however, is secondary to the broader normative implications of the surveillance. Mass surveillance, as noted previously, has chilling and moderating effects that are not resolved simply by rendering the surveillance 'transparent' (read - invisible) to individuals using the Internet. Moreover, by aggressively deploying such mass surveillance tools, individuals may modify their behaviours based on evident and non-evident uses of the technology. The very presence of mass-surveillance, regardless of its uses, can modify the willingness of individuals to communicate:[555] as such, DPI by its nature functions as a censor, a censor

---

[555] See: Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression," United Nations Human Rights Council Twenty-third session, agenda item 3, April 17, 2013, accessed August 30, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf; Sherry Turkle, Alone Together: Why we expect more from technology and less from each other (New York: Basic Books: 2011); Steve Henn, "Switching to Gmail May Leave Reporters' Sources At Risk," *NPR*, August 16, 2013, Accessed August 30, 2013, http://www.npr.org/blogs/alltechconsidered/2013/08/16/212678437/switching-to-gmail-may-leave-reporters-sources-at-risk.

that is damaging to the pursuit of pluralistic discourse over contemporary communications mediums.

While both surveillance and privacy operate as helpful tools in understanding the significance of DPI-based practices, it is only when turning to a model of democracy that focuses on the deliberative aspects of politics that it becomes apparent how significant these practices are. Privacy *supports* the broader concept of deliberative democracy, a mode of democracy that is inclusive, temporally considerate, open-ended, meant to accommodate difference, and predicated on free speech. Illegitimate surveillance, in contrast, undermines such a democratic ideal. The conclusion, however, is not that an inability to realize deliberative principles will *undermine* the potentiality of a democratic state, but that a particular kind of democratic state is challenged; as noted by Cohen, in the face of intensely anti-private practices a kind of 'modulated democracy' can develop. Such democracies are "emerging as networked surveillance technologies take root within democratic societies characterized by advanced systems of informational capitalism. Citizens within modulated democracies - citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests - increasingly will lack the ability to form and pursue meaningful agendas for human flourishing."[556]

DPI-driven practices that selectively limit or disrupt citizens' communications may be normatively coherent with such modulated democracies. These democracies might prioritize speed and safety of communications ahead of the democratic capacities or potentials of free speech, might emphasize the 'cost' of bad communications instead of the value of playful, unrestrained, and sometimes dangerous speech and digital association. As such, DPI and the associated practices of digital surveillance that are undertaken by corporations and government may be internally coherent with a form of political subjectivity that is more aligned with efficient distributions of data flows than with the dignity of individuals' communications. The terms to respond to this new subjectivity, however, do not necessarily emerge from a dominantly liberal or even republican approach to democracy: deliberative democratic theory provides a highly applicable normative analysis with pragmatic implications for action that can respond to

[556] Julie Cohen, "What Privacy Is For," *Harvard Law Review* 126: 1904 (2013), 1912.

– and counter – the anti-deliberative subjectivity linked with technocratic definitions or fiats of what constitutes 'good' and 'bad' speech. Though no normative argument or its accompanying practices will necessarily be successful in undermining contemporary modulated democracies, such arguments can help to reorient, redefine, and resist practices and ethics counter to deliberative principles at the foundation of most Western democratic constitutions.

Modulated democracies are fundamentally incompatible with deliberative democratic states, insofar as citizens in such states must be able to access, disseminate, and discuss information amongst one another and within various communities in which individuals claim membership. In the era of the Internet, such communities are often exclusively online, often depend on the dissemination of content or use of particular applications protocols, and are negatively affected by either commercial surveillance that limits communication or attempts to commoditize online communications,[557] and by government surveillance that chills speech and action.[558] It is critical that the existing culture of surveillance be reformed in order to protect and preserve the essential discursive foundations of our democracies.

Moderating DPI's Anti-Democratic Potentials

Though I have suggested that DPI-related practices may be incompatible with a deliberative democratic state, the effects of such practices can be moderated. In what follows, I outline how to rectify some of the power asymmetries between network controllers and subscribers controlling the ends of the network, to shift terms of 'surveillance consent', and to overhaul government surveillance behaviours. My discussion of these suggestions takes two tracks, insofar as I identify normative mechanisms to rectify deficiencies, and then briefly suggest practice(s) to realize those

---

[557] See: Sherry Turkle, *Alone Together: Why we expect more from technology and less from each other* (New York: Basic Books: 2011).

[558] This 'chilling effect' has been prominently demonstrated in 2013, with the closure of public law blogs and encrypted email communications systems. See: Katherine Jacobsen, "Tech law blog Groklaw shuts down, cites surveillance concerns," *The Christian Science Monitor*, August 21, 2013, Accessed August 30, 2013, http://www.csmonitor.com/Innovation/Responsible-Tech/2013/0821/Tech-law-blog-Groklaw-shuts-down-cites-surveillance-concerns. For a broader, international, discussion of how government surveillance chills speech see: Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression," United Nations Human Rights Council Twenty-third session, agenda item 3, April 17, 2013, accessed August 30, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

mechanisms. In aggregate, these suggestions, if implemented, would moderate the more destructive facets of DPI-related practices and facilitate the potentials of pluralistic deliberative democracies that depend on digital communications systems to generate political legitimacy.

Render Technologies Transparent

Deep packet inspection equipment is largely developed, 'standardized', and deployed outside of the purview of the international standards organizations. Though this is beginning to change - the International Telecommunications Union (ITU) recently published a draft of what the technology ought to be capable of - there has yet to be an open, transparent standards development process for the technology that is inclusive to all interested participants. 'Inclusivity' can assume a multitude of different forms, but at a minimum it should include non-engineering stakeholders, such as civil liberties and rights organizations, to identify and head off prospective public policy issues. These organizations can also inject 'public' values into the development processes themselves. Alongside such inclusivity efforts, there should be a public availability of relevant standards. Instead of sheltering how DPI appliances engage with data streams from public view, third-party experts who *are not* involved in the standards-setting process should be able to access standards so they can analyze, critique, lay bare their limitations and technical weaknesses, as well as identify unintended consequences or potentials for function creep. While these efforts to render DPI transparent do not necessarily empower 'typical' end-users, such as those who subscribe to Internet broadband services, they would enhance the abilities of civil society, government regulators, and interested corporate actors to more concisely debate the potentials and non-potentials of DPI appliances that conform to particular standards. Instead of DPI being regarded as a nebulous black box, it might be possible to raise the level of discourse concerning DPI and its associated practices and to adopt shared terms that have been collectively developed by multidisciplinary stakeholders during the standards-setting process itself.

The means of rendering DPI standards transparent need not be terribly invasive; doing so predominantly requires re-entrenching international standards bodies as key sites of standards development. Given the rate at which network technologies evolve today, a 'partial-Request For Comments (RFC)' track could be adopted to ensure that

developments were hashed out and even deployed prior to creating the 'finalized' standard. Equivalent efforts already exist, as demonstrated in the adoption of 'draft' versions of wireless communications protocols (e.g. 802.11a/ac/b/g/n). The direct involvement of informed members of civil society is a more challenging task, though one that can be overcome. Already, civil advocates are involved in standards organizations such as the IETF and W3C. These individuals bring a wealth of information beyond the technical details of the standard, and they could help to develop 'public policy impact assessments' to ascertain the broader potential implications of a standard related to DPI. As noted by Morris Jr., such assessments "must be in terms that are well understood by the community of technologists in the standards body"[559] and, as such, the assessment process would need to take public policy concerns and 'translate' them into actionable information that can be considered by technologists.

The by-product of these processes - both the rendering of standards as transparent and involvement of public advocates – would bring dimensions of deliberative power to bear on the technocratic development of digital equipment, insofar as the capability to simply *debate* the merits of the technology would be rendered more transparent and accessible. Such transparency and accessibility, however, would likely tend to require filters and further translation to the public. These proposals on their own would not correct the anti-democratic character of DPI equipment today. Nevertheless, increasing transparency vis-à-vis standards setting might raise the level of discourse amongst domestic stakeholders by establishing a common set of terms to debate, whilst also heading off potential applications of DPI that might lead to significant, unintended, public policy debacles.

Render Practices Transparent

Across cases, Internet service providers or governments often unilaterally began using DPI for specified practices and subsequently faced pushback from other policy actors and communities. ISPs and governments routinely withhold information about the specifics of how they were use the technology, the range of potential practices the technology

---

[559] John B. Morris Jr., "Injecting the Public Interest into Internet Standards," in *Opening Standards: The Global Politics of Interoperability*, edited by Laura DeNardis (Cambridge, Mass.: The MIT Press, 2001), 10.

could be used for, or the underlying economic, political, or securitization impetus(es) for adopting the practices linked with DPI. Moreover, the actors that deploy the technologies are routinely 'found out' instead of choosing to proactively declare how and why the technology is used ahead of adoption or deployment. The consequence is that the communications networks that individuals and communities rely on to conduct their economic, social, and political affairs are being modified without any involvement of those affected, to the effect that individuals' communications, associations, or practices may be compromised or modulated based on the network controllers' whims.

The practices linked to DPI should be rendered transparent in order for citizens and other members of society to publicly debate the merits of how network controllers interdict Internet subscribers' data packets. ISPs might be required to declare the present and possible uses of network interdiction equipment during relevant policy contestations. As an example, such a declaration might require outlining the full range of potential uses of traffic management equipment during telecommunications hearings about traffic management practices. ISPs could be compelled to produce quarterly or yearly statements of when and why their DPI-related practices led to complaints and the responses provided to complainants. Moreover, regulators could periodically run 'spot checks' to ensure that companies' stated uses of DPI equipment cohered with actual uses, with the regularity of such checks dependent on the number of complaints surrounding DPI-based practices an ISP garnered from its subscribers each year. All of these transparency actions could be mandated by legislative updates to telecommunications legislation where regulators lack the power to mandate such transparency actions.

Government actions could also be rendered more transparent. To begin, federal governments could issue privacy impact assessments that account for the mass surveillance capacities of specific instances of network-based packet monitoring. These assessments would be developed for each program using DPI and could be provided to relevant legislative oversight committees. Moreover, specialized watchdogs such as privacy commissioners as well as security and surveillance oversight commissioners could also be tasked to ensure that government surveillance actions were kept in check. These same watchdogs ought to be empowered to take legal action if government is found to be inappropriately, or illegally, conducting network-based surveillance. Finally,

governments could pass laws that better protected whistleblowers so that those who alert the public about secretive and overbearing government surveillance are not excessively punished.

The parties that control, or can take control of, the digital networks that citizens use on a regular basis have considerable potential to influence or monitor individuals' communications. By rendering these controllers' practices more transparent, and combined with rendering the technology itself more transparent, better public debate about specific uses of DPI might occur. In effect, the aim is to recognize that DPI equipment may be a useful technology to resolve specific issues while also making clear how and why the technology is used. The result of this transparency would be to maintain, or potentially restore, trust in the digital communications networks that citizens use on a regular basis.

Renewed Focus on Common Carriage

Internet service providers, as the chokepoints of communications flows, are central actors to any and all digital communications; as such, the potentialities of these companies' actions are even more far-reaching than the largest of Web-based companies. ISPs have aggregated so much control over communications over the past decade, at least in part, because the individuals using the Internet are often unable to make informed decisions concerning the reception or delivery of potential harmful, malicious, or otherwise detrimental network traffic.[560] The shift towards increasingly managing subscribers' Internet communications matters because "[c]onsciously or unconsciously, deliberately or inadvertently, societies choose structures for technologies that influence how people are going to work, communicate, travel, consume, and so forth over a very long time."[561] As was demonstrated in the previous chapter, the issue of who predominantly controls network flows has been a dominating characteristic of the DPI debates in the examined jurisdictions; a prolific group of civil society advocates, journalists, and other parties who represent the 'ends' of the network have repeatedly raised concerns that ISPs could shift

---

[560] Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven: Yale University Press, 2008), 45.
[561] Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago: The University of Chicago Press, 1986), 28.

control of communications traffic away from the ends of the networks to protect their business interests or extract rent from end-users.

Given that critics have cast suspicion upon ISPs and their often self-stated intentions or desires to deliberately interfere with traffic using DPI for non-network management purposes, a re-entrenchment of telecommunication common carrier rules could alleviate network users' concerns. The principle of common carriage was designed to prevent *network* owners from discriminating against service owners or users; owners can exclusively differentiate between transited packets for administrative purposes. Common carriage principles ensure that citizens and service providers can continue to communicate with one another without carrier interference and are based on a belief that, in the absence of regulation, carriers with sufficient monopoly power may discriminate against users of the network. However, common carriage principles have significantly been set aside as Western telecommunications markets have been liberalized; (re)entrenching common carriage demands that politicians either revisit telecommunications law *or* issue new policy statements to guide regulators toward regulatory decisions that adhere to common carriage. Given that discrimination using DPI can occur without end-users knowing *precisely* where the problem resides, it is essential that regulators be involved in overseeing any compliance with common carriage principles. Such oversight may demand increasing regulators' power to independently examine ISPs' practices and the justifications of such practices.

Though common carriage is ostensibly designed to prevent monopolists or oligopolists from discriminating against freighted material, it also (effectively) "protects ordinary citizens in their right to communicate."[562] This protection is accomplished by restricting how communications are discriminated against; while technologies such as DPI might be used for administrative network management (e.g. addressing particular kinds of network congestion) any additional kinds of discrimination would be largely barred. Moreover, common carriage principles can serve to shift what drives telecommunications policies more generally; whereas market liberalization has significantly set aside common carriage in an effort to ensure consumer "right of access"

---

[562] Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, Mass.: The Belknap Press of Harvard University Press, 1993), 106.

to telecommunications services, re-entrenching common carriage could lead to greater focuses on citizens' "right to communicate."[563] On the basis of common carriage, ISPs would be restricted in the degrees of communication surveillance and interdiction they could engage in. Though such restrictions would not entirely remove the experience of surveillance that citizens may experience when communicating online, they might make the nature, intent, and practices associated with the surveillance transparent; secretive or experimental uses of the technology would not be used to discriminate against communications or their content based on anything other than administrative demands. Ultimately, these principles would restrict the kinds of censorship while simultaneously reorienting telecommunications principles towards ensuring unhindered communications between citizens.

Reorientation of Notification and Consent Doctrines

Liberal conceptions of privacy tend to revolve around notions of informed consent, but any meaningful decision to consent to data collection or surveillance should include "some genuine alternatives and refusal costs that are not wildly exorbitant."[564] In the context of monopolistic and oligopolistic telecommunications markets, often with competitors that limit disclosure of how they use DPI, it can be challenging for consumers to understand how their provider interdicts telecommunications data. In markets characterized by ISPs that engage in common DPI-driven practices, consumers who *do* inform themselves may be unable to refuse to be monitored by the technology without (effectively) giving up access to Internet services. As a result, there is "no automatic, positive, link between knowledge and power, especially if that means power in a social or political sense … Of the many conditions that affect the phenomenon of power, knowledge is but one and by no means the most important."[565] The implication of this separation of knowledge and power to act is to bring into question the appropriateness of focusing on *individual* consent as the means of securing authorization

---

[563] Graham Longford, Marita Moll, and Leslie Regan Shade, "From the "Right to Communicate" to "Consumer Right of Access": Telecom Policy Visions from 1970-2007," in *For $ale to the Highest Bidder: Telecom Policy in Canada*, edited by Marita Moll and Leslie Regan Shade (Ottawa: Canadian Centre for Policy Alternatives), 6.

[564] Gary Marx, "Ethics for the New Surveillance," in *Visions of Privacy: Policy Choices for the Digital Age*, edited by Colin J. Bennett and Rebecca Grant (Toronto: University of Toronto Press), 52.

[565] Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago, The University of Chicago Press, 1989), 109-10.

for the collection, use, or transmission of personal information. As discussed earlier, network surveillance technologies have the effect of working on *populations* and privacy literatures – and laws – have tended to pose remedies from the perspective of individuals. As both individuals and populations can both be affected by DPI-based practices, renewed attention must be assigned to the link between actionable knowledge and meaningful informed consent of the individual.

As it stands, focusing on raising the digital literacy of individual consumers may not be the ideal 'target' group. Instead, legislators – not just regulators – must be brought up to speed so they understand how digital technologies intersect with existing democratic freedoms and associated rights. Such education or literacy efforts should include, as part of a broader program, attention to contemporary telecommunications infrastructure. Such infrastructure and its associated services are the 'tubes' responsible for much of the digital economy, and as such can be justified as sites of study. With an education on how contemporary digital systems operate and the means by which contemporary surveillance functions, legislators could actually engage in informed debate when they invigorate existing privacy laws to account for how mass surveillance practices do, or do not, infringe citizen's expectations of privacy. Such accounts of privacy ought to recognize the socialized nature of privacy, the capacity to derive significant degrees of information about individuals using 'non-personal' information, and the limited abilities of individuals to 'consent' to data collection practices that are opaque, opt-out, or that lack genuine conditions for individual consent.

Aligning privacy to both empower individuals *and* restrict the wholesale surveillance of populations has the effect of enabling individuals to engage in deliberative democratic practices. Undoubtedly, stronger and modernized privacy laws that secure individuals and populations from domestic state and corporate surveillance will reduce the censorious nature of the contemporary Internet ecosystem. At the same time, these new laws will also reorient privacy such that if contract remains the predominant way of securing consent, then consent would have to be genuinely received as opposed to the sham of contemporary 'consent'. The ultimate effect would be to renew trust in Internet intermediaries (and Internet-partners who individuals do business with online) and

remedy the secretive surveillance aspects of contemporary online life that may restrict our communications, actions, and associations.

Cessation of Secretive Government Surveillance

Secretive government surveillance has the effect of reducing trust in the actions of government whilst simultaneously drawing into question the consequences of citizens' actions that are (self-)regarded as not warranting the state's attention. Governments, such as those in the United States and United Kingdom, do not have a problem of obtaining data; instead, the current problem that DPI is used to solve is "deciding which data is worth analyzing and then interpreting it…Data collection is easy; analysis is difficult."[566] Presently, American and British intelligence services have deployed DPI and analyzed communications traffic using secretive interpretations of public law, but domestic and international persons' liberty and privacy have been infringed upon. That a machine was responsible for analyzing data – and not necessarily a human analyst – is no comfort. In an era where computer analyses can lead to life-changing experiences for individuals, the idea that the source of that change originated with a computer instead of with a person is cold comfort. Moreover, the secrecy surrounding the *practices* restricts public debate concerning the appropriateness, legality, and constitutionality of government-mandated surveillance practices. Such secrecy creates a chilling environment for anyone who personally believes – regardless of the 'truth' in the eyes of intelligence agencies – they must avoid saying, doing, or associating with a person or activity solely on the basis that they fear attracting the attention of intelligence and security services.

In the face of the significant secrecy around government surveillance practices, executive branches of government must be compelled by their legislative bodies to cease such activities. Special hearings and committees – bearing resemblance to the Church Committee that examined, and restrained, American intelligence activities in the 1970s – are needed to bring clarity to the range of the state's present behaviours and to restrain its actions. Admittedly, such hearings and committees will only take place once the democratic onus to investigate government surveillance exceeds legislators' own interests in satisfying security and commercial interests that support the legislators, and which

---

[566] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security In An Uncertain World* (United States: Springer, 2006), 162.

benefit from providing surveillance equipment and expertise to government. The value of such mechanisms is to render transparent the *practices* engaged in, not the specific persons that are monitored, the specific keywords examined, and so forth. To be clear, the divulgence of *practices* should not render legitimate security and intelligence measures moot: good security systems ought to be predicated on their continued operation in light of 'attackers' knowing how it works. The same can arguably be said for intelligence apparatuses. The knowledge of what government spies can do when in the field does not indicate who is, and is not, a government spy, but instead demonstrates to the public the range of actions that it – through its elected representatives – approves of.

Secret government surveillance poses significant threats to any concept of deliberative democracy on three separate fronts. First, it establishes a set of laws or interpretations of laws that the public cannot be reasonably believed to have legitimated. Without any knowledge of the law itself, or how it is interpreted, citizens cannot be said to have reasonably approved such a law. As a result, government acts outside of the scope of citizen-authorization when crafting or adhering to secret law, and it dangerously separates its own actions from the actions of the citizens; rather than citizens being the centre of democratic power, they become serfs to be protected by their governing representatives. Second, such surveillance has a chilling effect on the population, straining the willingness of deliberative participants to take part in 'risky' political debates that might – or might not – be monitored by government. And, given the breadth of communications surveillance that has been revealed in the United States, the extent to which individuals are monitored appears to be expansive. No state that genuinely supports deliberative democratic norms vis-à-vis strong rights of speech, association, or freedom from unwarranted searches can be expected to continue to thrive under such conditions. Finally, the current way that persons around the world are learning about the extent of secretive Western surveillance is the result of individuals engaging in whistleblowing. While such actions are important and provide a valuable way of entering information into the public domain for discussion, there should not be an expectation that individuals ought to violate the law (i.e. provide classified documents to members of the press or public) in order to learn about and constrain the actions of the state. Law

breaking cannot be regarded as a legitimate primary, secondary, or tertiary mechanism to structure government engagements with citizens or vice versa.

Ultimately, the effectiveness of these five suggestions remains unclear. Together, they are meant to resist shifts toward 'modulated democracies' that value efficient transfer of data over free speech, that permit algorithmic mass-surveillance as a default rather than as an exception. Combined, these suggestions would bring deliberative power to bear on the technocratic development of surveillance equipment, clarity into ISPs' and government's use of DPI equipment, weaken ISPs' legal capabilities to interdict and monitor their subscribers' communications, set the conditions for better privacy laws that could protect citizens' online speech and association, and restore legitimacy to government surveillance practices. In aggregate, these suggestions would better instantiate deliberative democratic norms into currently bureaucratic and technocratic policy forums that govern DPI-based practices, to the effect of reducing communicative surveillance and enhancing individuals' abilities to communicate without the present degrees of coercion. However, the technicity of modulated democracy may have already become so entrenched that such suggestions may be insufficient; instead of treating DPI and other mass surveillance technologies as needing 'moderation' it is possible that a more comprehensive excision of these technologies and associated practices is needed. In effect, it is possible that a political milieu compatible with modulated democracy may be on the rise, or have already arose, to the point where more radical proposals are required.

Next Research Steps

My research has established a foundation for subsequent, increasingly detailed, empirical and theoretical analyses of specific corporate practices that are related to telecommunications control and surveillance. Although I have laid bare the dimensions of network-centric control on wireline telecommunications networks, further work is needed to explore the full ramifications of such control in Western democratic states. In what follows, I conclude by outlining future lines of research that can continue to advance research into network surveillance and control.

Throughout this dissertation I have focused exclusively on wireline networks and the attempts of public and private interests to monitor those networks using deep packet inspection appliances. While I have focused on what has driven applications of DPI on

these networks, wireline networks – though important for mid-network bandwidth transportation – are increasingly the networks of the past. Mobile technologies and wireless broadband is a comparatively booming economic space that possesses significantly different technical characteristics than wireline networks. Such differences include perceived scarcities of bandwidth related to wireless spectrum limitations, challenges in managing signalling congestion between cellular towers and mobile devices, and the common challenge for mobile carriers to establish new cellular towers in under-provisioned urban areas. Moreover, while 'mobile' is presently understood by regulators to mean cellular phones and USB-powered broadband routers, as we move increasingly towards an 'Internet-of-Things' (IoT) the capacity to unilaterally affect the collection, dissemination, and reception of ambient sensor data will become increasingly important. The IoT heralds sensing networks that will be used to both automate the home and collect data for public policy and international environmental governance; the decisions made to affect such data streams, then, may have ramifications for consumers as well as for broader governance decisions. Given that mobile communications are already regarded as a 'more regulated' space, insofar as carrier providers often control what, and how, content is accessed and disseminated on such mobile networks, it will be critical to inspect the existing drivers in the mobile space and to understand how, and if, these drivers intersect with DPI-based network control and how any such intersection might affect the digitization of the physical world itself. Despite carriers' relative 'ownership' of how content is accessed and under what conditions, government regulators do nominally officiate the allocation of public spectrum, thus affording regulators the potential to condition how carriers interdict IoT-related content.

The capacity to monitor mobile communications does not just let corporate parties enhance control over the fastest-growing means of communication, nor next-generation sensing networks. In this dissertation, I have discussed how DPI is used for national security purposes in the United States and United Kingdom; it is important to understand how these governments rely on this technology in the course of capturing and interrogating mobile communications traffic. Moreover, given the prospect of extending sensor networks that will rely on wireless communications throughout the world, there is a very real possibility of expanded government surveillance capacities. Consequently a

further line of research will (effectively) carry out the methodology and structure of this dissertation, but to understand whether and how government DPI-driven surveillance is being applied to mobile communications systems.

This project has largely focused on the decisions concerning DPI that have been reached to date, but it has involved a less comparative analysis of the long-term implications of such decisions. Many of the institutional decisions discussed in this dissertation are very recent or, as of writing, coming into the public eye for the first time. As a result, the comparisons that have been drawn can be enhanced by a longitudinal evaluation of regulatory and political decisions. Will political decisions concerning the use of DPI hold in the face of public disclosures of state surveillance practices? Will regulations established in Canada be sufficiently applied to prevent ISPs from discriminating against wireless data traffic that is received by mobile devices? Will the political concessions surrounding copyright infringement be sufficient to placate rights holders, or will they (again) cast their gaze on DPI or similar data interdiction technologies to prevent the dissemination of prospectively infringement content? The advantage of a long-term analysis of these issues would be to better understand how regulatory and political branches of government maintain, enhance, or degrade existing decisions. Such insights could be contrasted against how and why decisions affecting digital surveillance and control technologies on wireline networks can be compared to regulatory and political discussions concerning other modes of surveillance. Moreover, this long-term comparison of DPI-related regulation and policies could better clarify how the existing decisions establish policy, technical, and legal 'frictions' that affect expansions of DPI-assisted surveillance.

Another line of research entails examining in more depth how DPI is, or can be, integrated with *domestic* law enforcement surveillance practices. A comparative project that contrasts Canada, the US, and other Western states' adoption or requirement of using DPI to capture communications content and metadata would be instructive in differentiating between predominantly national security/intelligence uses of DPI and how domestic federal, provincial, and municipal authorities could be, or are, enhancing their powers using DPI-driven surveillance capabilities. As revealed in my dissertation, Canadian telecommunications executives do not believe that DPI is presently required to

comply with lawful interception requirements, whereas the American situation suggests that intelligence-gathering applications of DPI have seen data routed to federal and state authorities.[567] It remains less clear, however, whether private companies might willingly disclose how their telecommunications networks are implicated with federal and state 'lawful intercept' capabilities. Nor is it clear whether government bodies could be compelled to disclose this information, short of new legislation being passed. Finally, it is unclear what variations might exist between legal and technical interception capabilities held by authorities in Canada and the United States. Given the relative dearth of scholarship that examines Canadian surveillance explicitly and the general reliance on American and other foreign states' practices to impute what occurs in Canada, exploring the direct relationship between domestic interception capabilities, legal requirements, and case law in Canada and other Western states could be used to ascertain common or dissonant approaches to using DPI for domestic interception. This exploration could also help to evaluate whether differences in technical measures of accessing data traffic for domestic purposes has a significant effect on the *practice* of accessing communications data for law enforcement purposes.

Finally, based on the influences of the ITU, IEFT, and W3C in the politics of deep packet inspection that were explored in this dissertation, future research could take up the role of the ITU based on its recent debates concerning DPI. The ITU's role could be contrasted against the influence of *regional* standards bodies that are predominantly involved in establishing lawful intercept and access capabilities into telecommunications equipment. Specifically, exploring the influence of European Telecommunications Standards Institute (ETSI) and ATIS (a North American telecommunications standards body) would be instructive, insofar as it might suggest the extent to which domestic government surveillance capacity emerges from a semi-private standards-setting environment rather than from the international bodies. Moreover, exploring whether decisions made in these regional bodies subsequently lead to moderations in states' bargaining positions or proposals at the ITU could suggest whether regional standards

[567] Jennifer Stisa Granick and Christopher Jon Sprigman, "NSA, DEA, IRS Lie About Fact That Americans Are Routinely Spied On By Our Government: Time For A Special Prosecutor," *Forbes*, August 14, 2013, accessed August 14, 2013, http://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/.

setting is functioning as a precursor to international standards setting, or vice versa, or whether the regional and international standards are largely separate from one another.

In summary, in this dissertation I have shone light into the murk of technical demands, business objectives, national security purposes, and regulatory processes to ascertain what has, and has not, driven the adoption of deep packet inspection in Canada, the US, and UK. DPI technologies are routinely heralded as either just the next logical step of packet inspection or as responsible for bringing an end to the Internet as we know it. In the course of evaluating the practices, regulations, and politics of DPI, it has become evident that neither bombastic position is entirely accurate. The development of packet inspection systems is continuing, but the adoption of DPI tends to be dependent on socio-political and economic conditions. Simply put, market demand is often a prerequisite for the technology's adoption by ISPs. The existence of such demand is no indication of the success of such technologies, however, because regulatory or political advocacy can result in the restriction or ejection of particular practices linked to the technology.

Across cases it became evident that DPI-related issues fell on separate, and not always parallel, regulatory or political policy streams. Most regulators tended to ultimately adopt similar principles, though arriving at such similarities was often the result of civil society and consumer advocates' work. Rarely was the fact that DPI operates as an explicit technology of control brought up by participating parties, although throughout the case studies it became apparent that similar policy communities across cases held common attitudes to whether network owners or Internet subscribers should control the flow, management, and reception of their data. These issues are temporarily settled, but they could arise anew. Recent revelations concerning mass state surveillance practices may prominently (re)open debates surrounding how DPI enables the surveillance and control of citizens' communications, but it is equally possible that there will only be limited and ineffectual efforts to drive back particular invasive uses of the technology. Ultimately, however, only longer-term study will reveal the extent to which DPI may reappear on the scene, and the extent to which the existing policy compromises will stick.

Technologies are deeply implicated in how we understand, engage with, and situate ourselves in the world, and DPI is no exception to this rule. The equipment used by ISPs is intended to expand the range of control over all communications that flow across the Internet, regardless of whether the communications are between individuals, between machines, or between machines and individuals. DPI lets network controllers intrude on communications and dictate the conditions under which they can be initiated, continued, or terminated. But the specificities of what deep packet inspection technologies enable are often unclear or misunderstood. But what is clear is that shifts concerning the control of communication threaten to profoundly affect the normative character of digitized deliberation in democratic states and, as such, it is imperative that the broader normative implications of DPI be raised in public political arenas. Regulatory arenas are insufficient domains for issues of this stake. In essence, the control afforded by DPI demands a robust political debate about the nature of free speech. After several years of regulators', courts', and limited legislatures' engagements with DPI-related practices, it is time that we have a proper debate about what is, and is not, an appropriate degree of corporate control over speech, action, and association over Internet-based communications. Doing anything less would demonstrate legislators' contempt for the communicative fabric of the contemporary Western democracies that they are elected to preserve.

Bibliography

80/80 Thinking Ltd. "First Stage (Interim) Privacy Impact Assessment for Phorm Inc." *The Guardian*, February 10, 2008. Accessed November 10, 2012. http://blogs.guardian.co.uk/technology/PhormPIAinterimfinal.pdf.

Abbate, Jennifer. *Inventing the Internet.* Cambridge, Mass.: The MIT Press, 1999.

Abbott, Kenneth W. and Duncan Snidal. "Hard and Soft Law in International Governance." *International Organizations* 54(3) (2000): 421-456.

Albanesius, Chloe. "Comcast Cuts Off Bandwidth Hogs." *PC Magazine*, April 4, 2007. Accessed May 17, 2013. http://www.pcmag.com/article2/0,2817,2111373,00.asp.

Alcatel-Lucent. "Traffic Management and 'Net Neutrality': A response from Alcatel-Lucent to the Ofcom consultation." *Ofcom*, September 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/AlcatelLucent.pdf.

Alder, Emanuel and Peter M. Haas. "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program." *International Organization* 46(1) (1992): 367-390.

Alter, Karen J., and Sophie Meunier. "The Politics of International Regime Complexity," *Perspectives on Politics* 7(1) (2009): 13-24.

Allot Communications. "Digging Deeper Into Deep Packet Inspection (DPI)." Allot, 2007. Accessed July 28, 2011. https://www.dpacket.org/articles/digging-deeper-deep-packet-inspection-dpi.

American Civil Liberties Union. "ACLU Files Lawsuit Challenging Constitutionality of NSA Phone Spying Program." *ACLU website*, June 11, 2013. Accessed September 7, 2013. https://www.aclu.org/national-security/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program.

Anderson, Nate and Eric Bangeman. "Comcast loses P2P religion, goes agnostic on throttling." *Ars Technica*, September 19, 2008. Accessed January 30, 2013. http://arstechnica.com/uncategorized/2008/09/comcast-loses-p2p-religion-goes-agnostic-on-throttling/.

Anderson, Nate. ""Canada: ISP traffic shaping should only be "last resort"." *Ars Technica*, October 21, 2009. Accessed September 9, 2013. http://arstechnica.com/tech-policy/2009/10/canada-isp-traffic-shaping-should-only-be-last-resort/.

Anderson, Nate. "Vendor throws DPI under the bus, says ISP deployment "risky"." *Ars Technica*, October 30, 2008. Accessed June 13, 2013.

http://arstechnica.com/uncategorized/2008/10/vendor-throws-dpi-under-the-bus-says-isp-deployment-risky/.

Anderson, Nate. "NebuAd CEO defends web tracking, tells Congress its legal." *Ars Technica,* July 9, 2008. Accessed March 2, 2013. http://arstechnica.com/tech-policy/2008/07/nebuad-ceo-defends-web-tracking-tells-congress-its-legal/.

Anderson, Nate. "White House: we "win the future" by making ISPs into copyright cops." *Ars Technica,* July 7, 2011. Accessed March 4, 2013. http://arstechnica.com/tech-policy/2011/07/white-house-we-win-the-future-by-making-isps-into-copyright-enforcers/.

Anderson, Nate. "ISPs: don't blame us; NebuAd did all the dirty work!" *Ars Technica*, February 6, 2009. Accessed February 7, 2013. http://arstechnica.com/tech-policy/2009/02/isps-who-used-nebuad-hey-they-did-all-the-dirty-work/.

Anderson, Nate. "Hammer drops at last: FCC opposes Comcast P2P throttling." *Ars Technica*, July 25, 2008. Accessed January 30, 2012. http://arstechnica.com/uncategorized/2008/07/hammer-drops-at-last-fcc-opposes-comcast-p2p-throttling/.

Anderson, Nate. "Deep Packet Inspection meets 'Net neutrality, CALEA." *Ars Technica*, July 25, 2007. Accessed March 20, 2011. http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars

Anderson, Nate. "Can ISPs charge more to make gaming less laggy? They already do." *Ars Technica*, December 15, 2010. Accessed March 22, 2013. http://arstechnica.com/tech-policy/news/2010/12/can-isps-charge-more-to-make-gaming-work-better-they-already-do.ars.

Anderson, Nate. "Oops: major Canadian ISP admits throttling *World of Warcraft.*" *Ars Technica*, March 29, 2011. Accessed June 20, 2012. http://arstechnica.com/tech-policy/news/2011/03/oops-major-canadian-isp-admits-throttling-world-of-warcraft.ars.

Anderson, Nate. "Imagine a world where every app has its own data plan." *Ars Technica*, December 15, 2010. Accessed March 22, 2013. http://arstechnica.com/tech-policy/news/2010/12/net-neutrality-nightmare-a-world-where-every-app-has-its-own-data-plan.ars

Anderson, Nate. "Major ISPs agree to "six strikes" copyright enforcement plan." *Ars Technica*, July 7, 2011. Accessed September 8, 2013 http://arstechnica.com/tech-policy/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan/.

Arbor Ellacoya. "Arbor Ellacoya e100: Unmatched Scale and Intelligence in a Broadband Optimization Platform (Datasheet)." Arbor Networks, 2009. Accessed March 14, 2011.

http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=355.

Arbor Networks, Inc. "From: Kurt Dobbins (kdobbins@arbor.net) on behalf of Arbor Networks, Inc. (Arbor) – Re: 2008-19-2." *CRTC,* February 24, 2009. Accessed Mach 23, 2012. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1032115.PDF.

ARCH. "Telecom Public Notice CRTC 2009-19 – Review of Internet Traffic Management Practices of Internet Service Providers: Oral Presentation." *CRTC*, July 8, 2009. Accessed March 23, 2012. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241696.PDF.

Asghari, Hadi, Mechel van Eeten, and Milton Mueller. "Unraveling the Economic and Political Drivers of Deep Packet Inspection: An empirical study of DPI use by broadband operators in 75 countries." Paper presented at GigaNet 7th Annual Symposium, Baku, Azerbaijan, November 5, 2012.

Atkinson, Michael M. and William D. Coleman. "Policy Networks, Policy Communities and the Problems of Governance." *Governance: An International Journal of Policy and Administration* 5(2) (1992): 154-180.

AT&T. "Re: Request for IPEC for Public Comments Regarding the Joint Strategic Plan (Fed. Reg. Vol. 75, No. 35 – FR Doc. 2010-3539)." *Whitehouse.gov*, March 24, 2010. Accessed March 4, 2013. http://www.whitehouse.gov/sites/default/files/omb/IPEC/frn_comments/AT_T.pdf.

Baker, Jennifer. "EU drops ePrivacy case against UK government." *Computer World UK*, published January 26, 2012. Accessed May 2, 2013. http://www.computerworlduk.com/news/public-sector/3332941/eu-drops-eprivacy-case-against-uk-government/.

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

BBC News. "Edward Snowden: Leaks that exposed US spy programme." *BBC News*, October 25, 2013. Accessed October 29, 2013. http://www.bbc.co.uk/news/world-us-canada-23123964.

BBC News. "EU to assess piracy detection software." *BBC News*, January 26, 2010. Accessed November 10, 2012. http://news.bbc.co.uk/2/hi/8480699.stm.

BBC News. "Open Rights Group questions Phorm." *BBC News*, March 12, 2008. Accessed May 10, 2013. http://news.bbc.co.uk/2/hi/technology/7291637.stm.

BBC. "BBC response to Ofcom's discussion document on traffic management and 'net neutrality'." *Ofcom*, September 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/BBC.pdf.

Beck, Ulrich. *World Risk Society*. Cambridge, UK: Polity, 1998.

Bell Aliant/Bell Canada (Bell). "Telecom Public Notice CRTC 2008-19, Review of Internet management practices of Internet providers (PN 2008- 19) – Comments." *CRTC*, February 23, 2009. Accessed June 28, 2009. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/102980 4.zip.

Bendrath, Ralf and Milton Mueller. "The End of the Net as We Know It." *New Media & Society* 13(7) (2011): 1142-1160.

Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* New Haven: Yale University Press, 2006.

Berners-Lee, Tim, with Mark Fischetti. *Weaving the Web: The original design and ultimate destiny of the world wide web.* New York: Harper Business Press, 2000.

Bill C-552. *An Act to amend the Telecommunications Act (Internet Neutrality)*, 2d sess., 39th Parliament, 2008. http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?billId=3463800&Language=E&Mode=1

Birkland, Thomas A. *After Disaster: Agenda Setting, Public Policy, and Focusing Events.* Washington, D.C.: Georgetown University Press, 1997.

Bivio Networks and Solera Networks. "White Paper: Complete Network Visibility through Deep Packet Inspection and Deep Packet Capture." Solera Networks. Lindon, Utah: Solera, 2008. www.soleranetworks.com/products/documents/dpi_dpc_bivio_solera.pdf.

Blumenthal, Marjory S. and David D. Clark. "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World." In *Communications Policy in Transition: The Internet and Beyond*, edited by Benjamin M. Compaine and Shane Greenstein, 91-139. Cambridge, Mass: The MIT Press, 2001.

Boam, Christopher and Vikram Raval (Verizon). "Commons of Verizon Communications In the U.K. Ofcom Public Consultation on "Traffic Management and 'Net Neutrality': a Discussion Document." *Ofcom*, issued June 24, 2010. Accessed November 19, 2012. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Verizon.pdf.

Bode, Karl. "Rogers' New Throttling System Cripples Speeds And inadvertently impacting non-P2P applications." *DSL Reports*, December 14, 2010. Accessed June 20, 2012.

http://www.dslreports.com/shownews/Rogers-New-Throttling-System-Cripples-Speeds-111830.

Bohm, Nicholas. "The Phorm "Webwise" System – a Legal Analysis." *FIPR*, April 23, 2008. Accessed May 10, 2013. http://www.fipr.org/080423phormlegal.pdf.

Bohm, Nicholas, and Richard Clayton. "Open Letter to the Information Commissioner." *FIPR*, March 17, 2008. Accessed May 10, 2013. http://www.fipr.org/080317icoletter.html.

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

BT. "BT Response to Ofcom Consultation on Traffic Management." *Ofcom*, issued September 9, 2010. Accessed November 19, 2012. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/BT.pdf.

BT Retail Technology. "PageSense External Technical Validation," *Wikileaks*, January 15, 2007, released on Wikileaks June 4, 2008. Accessed November 2012. http://wikileaks.org/wiki/British_Telecom_Phorm_PageSense_External_Validation_report.

Campaign for Democratic Media. "Oral Submissions of Campaign for Democratic Media – Telecom Public Notice CRTC 2008-19: Review of the Internet Traffic Management Practices of Internet Service Providers." *CRTC*, July 9, 2009. Accessed March 3, 2012. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241703.PDF.

The Canadian Film and Television Production Association and the Independent Film and Television Alliance. "Oral Remarks by The Canadian Film and Television Production Association and the Independent Film and Television Alliance - Telecom Public Notice CRTC 2008-19 – Review of Internet traffic management practices of Internet service providers." *CRTC*, July 8, 2009. Accessed March 4, 2012. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241693.PDF.

Castro, Daniel, Richard Bennett, and Scott Andes. "Steal These Policies: Strategies for Reducing Digital Piracy." *The Information Technology & Innovation Foundation,* December 2009. Accessed February 27, 2013. http://www.itif.org/files/2009-digital-piracy.pdf.

CBC News. "Online surveillance bill setup costs estimated at $80M." *CBC News: Politics*, February 22, 2012. Accessed April 9, 2012. http://www.cbc.ca/news/politics/story/2012/02/22/pol-lawful-access-costs.html.

CBC News. "Online surveillance bill backed by police chiefs." *CBC News: British Columbia*, February 20, 2012. Accessed June 22, 2012. http://www.cbc.ca/news/canada/british-columbia/story/2012/02/20/bc-police-bill-c-30.html.

Center for Democracy & Technology. "An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd system and Other Uses of Internet Traffic Content from ISPs for Behavioural Advertising." *Center for Democracy and Technology,* July 8, 2008. Accessed February 6, 2013. https://www.cdt.org/privacy/20080708ISPtraffic.pdf.

Cerf, Vint and Bob Kahan. "A Protocol for Packet Intercommunication." *IEEE Transactions on Communications* 22(5) (1974): 637-648.

Chambers, Simone. "Deliberative Democratic Theory." *Annual Review of Political Science* 6 (2003): 307-326.

Chase, Steven. "Ottawa hits pause on Web surveillance act." *The Globe and Mail,* February 24, 2012. Accessed March 28, 2012. http://www.theglobeandmail.com/news/politics/ottawa-hits-pause-on-web-surveillance-act/article2349818/page1/.

Chilling Effects Clearinghouse. "DMCA Safe Harbour." *Chilling Effects Clearinghouse*. Accessed May 10, 2013. https://www.chillingeffects.org/dmca512/.

CIPPIC. "Re: Bell Canada/Bell Sympatico Use of Deep Packet Inspection: PIPEDA Complaint." *CIPPIC*, May 9, 2008. Accessed May 12, 2013. http://www.cippic.ca/sites/default/files/Bell-DPI-PIPEDAcomplaint_09May08.pdf.

CIPPIC. "ISP Use Of Deep Packet Inspection (May/July 2008)." *CIPPIC*, updated September 2010. Accessed May 12, 2012. http://www.cippic.ca/en/DPI.

CIPPIC. "What is "lawful access?" *CIPPIC*, last updated June 2, 2007. Accessed March 22, 2013. http://www.cippic.ca/en/lawful-access-faq.

CIPPIC. "Supplement Letter to Complaint #6100-02744." *CIPPIC,* May 26, 2008. Accessed May 12, 2013. http://www.cippic.ca/sites/default/files/Bell-PIPEDAsup1-behavioural%20targeting_26May08.pdf.

CIPPIC/CDM. "In The Matter of an Application by The Canadian Association Of Internet Providers ("CAIP") (Applicant) Pursuant To Part VII Of The CRTC Telecommunications Rules of Procedure and Sections 7, 24, 25, 27, 32, 36, And 62 of the Telecommunications Act directed to Bell Canada (Respondent) Requesting Certain Orders Directing Bell Canada to Cease and Desist From "Throttling" Its Wholesale ADSL Access Services Comments of the Campaign for Democratic Media ("CDM")." *CRTC*, July 3, 2008. Accessed April 22, 2012. http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923867.zip.

Cisco. "Introduction to Cisco MPLS VPN Technology," in *MPLS Solution User Guide*. Accessed June 26, 2011.

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html.

Cjhort. "[HSI] Charter to monitor surfing, inserts its own targeted ads." *Broadband DSL Reports* (forum), May 10, 2008. Accessed February 5, 2013. https://secure.dslreports.com/forum/r20461817-HSI-Charter-to-monitor-surfing-insert-its-own-targeted-ads.

Clarke, Roger. "Introduction to Dataveillance and Information Privacy, and Definitions of Terms." *Roger Clarke's Web-Site*, August 7, 2006. Accessed August 9, 2013. http://www.rogerclarke.com/DV/Intro.html.

Clarke, Roger. "Information Technology and Dataveillance." *ACM* 31(5) (1988): 498-512.

Clarke, Rogers. "Information Technology and Dataveillance." *Roger Clarke's Website*, 1987. Accessed March 25, 2013. http://www.rogerclarke.com/DV/CACM88.html#PDV.

Clayton, Mark. "Snowden leaks give new life to lawsuits challenging NSA surveillance programs." *The Christian Science Monitor*, July 18 2013. Accessed September 7, 2013. http://www.csmonitor.com/USA/Justice/2013/0718/Snowden-leaks-give-new-life-to-lawsuits-challenging-NSA-surveillance-programs.

Clayton, Richard. "Stealing Phorm Cookies." *Light Blue Touchpaper*, April 22, 2008. Accessed May 10, 2013. http://www.lightbluetouchpaper.org/2008/04/22/stealing-phorm-cookies/.

Clayton, Richard. "What does Detica detect?" *Light Blue Touchpaper*, December 7, 2009. Accessed November 11, 2012. http://www.lightbluetouchpaper.org/2009/12/07/what-does-detica-detect/.

Clayton, Richard. "The Phorm "Webwise" System," last revised May 18, 2008. Accessed March 22, 2013. http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

Cogeco. "CRTC File No: 8646-C12-200815400 - Telecom Public Notice CRTC 2008-19, Review of the Internet traffic management practices of Internet service providers - Cogeco Reply Comments," *CRTC*, April 30, 2009. Accessed June 28, 2009. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/111048 8.pdf.

Cohen, Julie. "What Privacy Is For." *Harvard Law Review* 126 (2013): 1904-1933.

Cohen, Julie. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52 (5) (2000): 1373-1438.

Comcast. "In the Matter of Broadband Industry Practices – WC Docket No. 07-52," *FCC*, February 12, 2008. Accessed June 19, 2013. http://apps.fcc.gov/ecfs/document/view?id=6519840991.

Computer Professionals for Social Responsibility. "CPSR Statement on the Computer Virus." *Communications of the ACM 32(6)* (1989): 507-508.

Consumer Focus. "Consumer Focus response to Ofcom's discussion paper on Net neutrality and traffic management." *Consumer Focus*, September 2010. Accessed May 12, 2013. http://www.consumerfocus.org.uk/assets/1/files/2009/06/Consumer-Focus-response-to-Ofcom-consultation-on-net-neutrality.pdf.

Cooper, Alissa. "UK Traffic Management Policies." *Alissa Cooper* (personal website), August 12, 2010. Accessed November 7, 2012. http://www.alissacooper.com/2010/08/12/uk-traffic-management-policies/.

Cooper, Alissa. "The singular challenge of ISP use of deep packet inspection." *Deep packet inspection Canada*, 2010. Accessed January 3, 2013. http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deeppacket-inspection/.

Cooper, Alissa. "The Next Tim Berners-Lee: Response to Ofcom Discussion on Traffic Management and Net Neutrality." *Ofcom*, September 9, 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Cooper_A.pdf.

Cowhey, Peter F. "The International Telecommunications Regime: The Political Roots of Regimes for High Technology." *International Organization* 44(2) (1990): 169-199.

Cranor, Lorrie Faith. *Web Privacy and P3P.* Sebastopol, CA: O'Reilly & Associates Inc, 2002.

Crawford, Susan. *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age.* New Haven: Yale University Press, 2013.

The Crown Prosecution Service. "CPS decides no prosecution of BT and Phorm for alleged interception of browser data." *The blog of the Crown Prosecution Service*, April 8, 2011. Accessed May 7, 2013. http://blog.cps.gov.uk/2011/04/no-prosecution-of-bt-and-phorm-for-alleged-interception-of-browsing-data.html.

CRTC. "Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers." *CRTC*, October 21, 2009. Accessed May 12, 2013. http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm.

CRTC. "Re: File 545613, Internet Traffic Management Practices ("ITMP"), Section 36 of the Telecommunications Act, S.C. 1993, c. 38, as amended ("Act"), and Paragraphs 126 and 127 of Telecom Regulatory Policy CRTC 2009-657 ("TRP CRTC 2009-657")" *CRTC*, January 20, 2012. Accessed June 20, 2012. http://www.crtc.gc.ca/eng/archive/2012/lt120120.htm.

CRTC. "Telecom Decision CRTC 2008-108." *CRTC*, November 20, 2008. Accessed May 12, 2013. http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm.

CRTC. "Telecom Regulatory Policy CRTC 2009-34." *CRTC*, 2009. Accessed Mary 12, 2013. http://www.crtc.gc.ca/eng/archive/2009/2009-34.htm.

Dahlberg, Lincoln. "The Internet and Democratic Discourse: Exploring the prospects of online deliberative forums extending the public sphere." *Information, Communications & Society* 4:4 (2001): 615-633.

Daly, Angela. "The legality of deep packet inspection." Paper presented at the First Interdisciplinary Workshop on Communications Policy and Regulation "Communications and Competition Law and Policy—Challenges of the New Decade," Glasgow, Scottland, June 17 2010.

Davies, Simon. "The conflict of interest – our response." *The Guardian*, March 19, 2008. Accessed November 10, 2012. http://www.guardian.co.uk/technology/blog/2008/mar/18/phormsreportfrom8020readi.

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

Defendants' Memorandum of Law in Support of Motion for Judgment on the Pleadings at 6, Hart v. Comcast of Alameda, No. C-07-06350-PJH (N.D. Cal. Mar. 14, 2008) (Comcast Motion for Judgment)

DeGeest, Kelly. "What is an MPLS VPN Anyway?" *SANS Institute*, 2001. Accessed June 25, 2011. http://www.sans.org/reading_room/whitepapers/vpns/mpls-vpn-anyway_718.

Deibert, Ron. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013.

Denardis, Laura. *Protocol Politics: The Globalization of Internet Governance*. Cambridge, Mass.: The MIT Press, 2009.

Detica. "Traffic Management and 'net neutrality." *Ofcom*, September 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Detica.pdf.

Dolowitz, David P. and David March. "Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making." *Governance: An International Journal of Policy and Administration* 13(1) (2000): 5-23.

Drake, William J. "Memo #3: ICT Global Governance and the Public Interest: Infrastructure Issues." For the Social Science Research Council's Research Network on IT and Governance, 2004.

Eckersly, Peter, Fred von Lohmann, and Seth Schoen. "Packet Forgery By ISPs: A Report on the Comcast Affair." *EFF*, November 28, 2007. Accessed January 30, 2013. https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

Eckersley, Peter. "FCC Hearings at Stanford: Towards a Consensus on ISP Transparency?" *EFF*, published April 18, 2008. Accessed May 13, 2013. https://www.eff.org/deeplinks/2008/04/fcc-hearings-stanford-consensus-isp-transparency.

Electronic Frontier Foundation. "Al Haramain v. Obama." *Electronic Frontier Foundation,* August 29, 2012. Accessed March 4, 2013. https://www.eff.org/cases/al-haramain.

enigma. "Virgin Media CEO Says Net Neutrality is "A Load of Bollocks"." *TorrentFreak*, April 13, 2008. Accessed November 8, 2012. http://torrentfreak.com/virgin-media-ceo-says-net-neutrality-is-a-load-of-bollocks-080413/.

Ernesto. "Rogers' BitTorrent Throttling Experiment Goes Horribly Wrong." *TorrentFreak*, December 13, 2010. Accessed June 21, 2012. http://torrentfreak.com/rogers-bittorrent-throttling-experiment-goes-horribly-wrong-101213/.

Esguerra, Richard. "Charter Communications ISPs Halts Traffic Inspection/Advertising Plan." *EFF*, July 25, 2008. Accessed June 13, 2013. https://www.eff.org/de/deeplinks/2008/06/charter-communications-isp-halts-traffic-inspectio.

Espiner, Tom. "Berners-Lee says no to internet 'snooping'." *ZDnet UK,* March 11, 2009. Accessed March 25, 2013. http://www.zdnet.co.uk/news/security-management/2009/03/11/berners-lee-says-no-to-internet-snooping-39625971/.

European Parliament and of the Council. "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive." *Official Journal L 105, 13/04/2006 P. 0054 – 0063*.

Farber, David J. "NSF Poses Code of Networking Ethics," *Communications of the ACM 32(6)* (1989): 505-506.

Farivar, Cyrus. "Here's what an actual "six strikes" copyright alert system looks like." *Ars Technica*, February 27, 2013. Accessed March 4, 2013. http://arstechnica.com/tech-policy/2013/02/heres-what-an-actual-six-strikes-copyright-alert-looks-like/.

Federal Communications Commission. "FCC 08-183: Memorandum Opinion and Order." *FCC,* August 20, 2008. Accessed August 23, 2013. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf.

FCC. *FCC 05-151 Internet Policy Statement*, adopted August 5, 2005. Accessed May 17, 2013. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

Fernandez, Ben. "Comcast Admits Paying Attendees at FCC Hearing." *The Philadelphia Enquirer*, February 28, 2008. Accessed May 15, 2013. https://www.commondreams.org/archive/2008/02/28/7355.

Finnie, Graham. "(Report) ISP Traffic Management Technologies: The State of the Art." *CRTC*, 2009. Accessed June 27, 2011. http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm.

Fisher, Ken. "BSA doesn't think the DMCA goes far enough." *Ars Technica,* January 7, 2005. Accessed May 1, 2013. http://arstechnica.com/uncategorized/2005/01/4511/.

Floyd, Sarah. "RFC 3360: Inappropriate TCP Resets Considered Harmful." *IETF*, August, 2002. Accessed March 25, 2013. http://www.ietf.org/rfc/rfc3360.txt?number=3360.

Free Press and Public Knowledge v. Comcast, 2008, FCC 08-183.

Fulton III, Scott M. "Comcast may get legal leverage to stop net neutrality enforcement." *Betanews*, January 9, 2010. Accessed May 2, 2013. http://betanews.com/2010/01/09/comcast-may-get-legal-leverage-to-stop-net-neutrality-enforcement/.

Fuchs, Christian. "Working Paper: Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society." EU FP7 – The Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research Into Action, July 2012.

Gabbatt, Adam. "'Nobody is listening to your calls': Obama's evolution on NSA surveillance." *The Guardian,* August 8, 2013. Accessed October 29, 2013, http://www.theguardian.com/world/2013/aug/09/obama-evolution-nsa-reforms.

Geist, Michael. "CWTA Calls on Government to Use Spectrum Auction Proceeds to Pay for Lawful Access." *MichaelGeist.ca*, April 3, 2013. Accessed April 9, 2013. http://www.michaelgeist.ca/content/view/6816/125/.

Geist, Michael. "Canada's Net Neutrality Enforcement Failure." *Michael Geist,* July 8, 2011. Accessed June 27, 2012. http://www.michaelgeist.ca/content/view/5918/159/.

Geist, Michael. "Lawful Access is Dead (For Now): Government Kills Bill C-30." *MichaelGeist.ca*, February 12, 2013. Accessed April 9, 2013. http://www.michaelgeist.ca/content/view/6782/125/.

Gettys, Jim. "Bufferbloat: Dark Buffers in the Internet." *IEEE Internet Computing* 15(3) (2011): 1-15.

Gilbert, Daphne. "Privacy's Second Home: Building a New Home for Privacy Under Section 15 of the Charter." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock. Toronto: Oxford University Press, 2009.

Goldsmith, Jack and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World.* Toronto: Oxford University Press, 2006.

Google. "Comments concerning CAIP Part VII Application requesting certain orders directing Bell Canada to cease and desist from "throttling" its wholesale ADSL Access Services." *CRTC,* July 3, 2008. Accessed March 3, 2012. http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923481.pdf.

Government of Canada. "Telecommunications Act." S.C. 1993, c. 38. http://laws-lois.justice.gc.ca/eng/acts/T-3.4/page-2.html#h-6.

Graber, Mark A., Donna M. D'Alessandro, and Jill Johnson-West. "Reading Level of Privacy Policies on Internet Health Websites." *Journal of Family Practice* 51(7) (2002): 642-645.

Graham, Paul. "The Submarine." *Paul G*, accessed March 22, 2013. http://www.paulgraham.com/submarine.html#f4n.

Granick, Jennifer Stisa and Christopher Jon Sprigman. "NSA, DEA, IRS Lie About Fact That Americans Are Routinely Spied On By Our Government: Time For A Special Prosecutor." *Forbes*, August 14, 2013. Accessed August 14, 2013. http://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/.

Gune, Dick, and Ceriel J.H. Jacobs. *Parsing Techniques: A Practical Guide.* West Sussex: Ellis Horwood Limited, 1990.

Habermas, Jürgen. "A Genealogical Analysis of the Cognitive Content of Morality." In *The Inclusion of the Other: Studies in Political Theory*, edited by Ciaran Cronin and Pablo De Greiff. Cambridge, Mass.: The MIT Press, 1998.

Habermas, Jürgen. "Three Normative Models of Democracy." In *The Inclusion of the Other: Studies in Political Theory,* edited by Ciaran Cronin and Pablo De Greill. Cambridge, Mass.: The MIT Press, 1998.

Hafner, Katie, and David Lyon. *Where Wizards Stay Up Late: The Origins Of The Internet.* Simon & Schuster, 1998.

Haggerty, Kevin D. and Richard V. Ericson. "The New Politics of Surveillance and Visibility." In *The New Politics of Surveillance and Visibility,* edited by Kevin D. Haggerty and Richard V. Ericson. Toronto: University of Toronto Press, 2007.

Hajer, Maarten and Wytske Versteeg. "A decade of discourse of environmental politics: Achievements, challenges, and perspectives." *Journal of Environmental Policy & Planning* 7(3) (2006): 175-184.

Hallman, Ben. "NSA Sued By Unusual Coalition Of Gun Rights And Environmental Activists Over 'Dragnet Surveillance'." *Huffington Post*, July 16, 2013. Accessed September 7, 2013. http://www.huffingtonpost.com/2013/07/16/nsa-sued-dragnet-surveillance_n_3605104.html?ir=Technology.

Hansell, Saul. "NebuAd Observes 'Useful, but Innocuous' Web Browsing." *New York Times Bits* (blog), April 7, 2008. Accessed February 5, 2013. http://bits.blogs.nytimes.com/2008/04/07/nebuad-observes-useful-but-innocuous-web-browsing/.

Harris, Shane. *The Watchers: The Rise of America's Surveillance State.* New York: The Penguin Group, 2010.

Henn, Steve. "Switching to Gmail May Leave Reporters' Sources At Risk." *NPR*, August 16, 2013. Accessed August 30, 2013. http://www.npr.org/blogs/alltechconsidered/2013/08/16/212678437/switching-to-gmail-may-leave-reporters-sources-at-risk.

Higginbotham, Stacey. "NebuAd Bites the Dust." *Gigaom,* May 19, 2009. Accessed February 7, 2009. http://gigaom.com/2009/05/19/nebuad-bites-the-dust/.

Hochheiser, Harry. "Indirect Threats to Freedom and Privacy: Governance of the Internet and the WWW." In *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions,* 2000, 249-254.

Hogge, Becky. "The Phorm Storm." *Open Rights Group*, March 12, 2008. Accessed May 10, 2013. http://www.openrightsgroup.org/blog/2008/the-phorm-storm.

Home Office. "Protecting the Public in a Changing Communications Environment: Summary of Responses to the 2009 Consultation Paper." *Home Office*, November 2009. Accessed May 12, 2013. http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary.

Hosein, Ian and Johan Eriksson. "International policy dynamics and the regulation of dataflows: bypassing domestic restrictions." In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello. New York: Routledge, 2007.

Howlett, Michael, and M. Ramesh. *Studying Public Policy: Policy Cycles and Policy Subsystems.* Toronto: Oxford University Press, 2003.

Interactive Advertising Bureau of Canada. "Comments Concerning - #: 8622-C51-200805153 - Canadian Association of Internet Providers (CAIP) - Application requesting certain orders directing Bell Canada to cease and desist from throttling its wholesale ADSL Access Services." *CRTC*, July 3, 2008. Accessed March 20, 2012. http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923856.zip.

IESG Secretary. "The IETF's position on technology to support legal intercept." IETF mailing lists, October 11, 1999. Accessed March 29, 2013. http://cryptome.org/ietf-snoop.htm.

Information Commissioners Office. "Phorm Advertising – ICO Statement." *Information Commissioner's Office*, April 4, 2008. Accessed May 1, 2013. http://www.ico.org.uk/upload/documents/pressreleases/2008/new_phorm_statement_040408.pdf.

Information Commissioner's Office. "ICO Statement on the Communications Data Bill." *Information Commissioner's Office*, 20 October 2008. Accessed May 12, 2013. http://www.ico.gov.uk/upload/documents/pressreleases/2008/ico_statement_comms_data_bill.pdf.

Information Sciences Institute (Jon Postel, editor). "RFC 793: Transmission Control Protocol DARPA Internet Program Protocol Specification." *IETF*, September 1981. Accessed March 25, 2013. http://www.ietf.org/rfc/rfc0793.txt.

Internet Activities Board. "Ethics and the Internet." *Communications of the ACM 32(6)* (1989).

Internet Architecture Board. "A Brief History of Internet Advisory/Activities/Architecture Board." IAB Website, 2011. Accessed March 25, 2013. http://www.iab.org/about/history/.

ISPA. "ISPA Response to the Ofcom Traffic Management Discussion Paper." *Ofcom*, issued 2010. Accessed November 19, 2012. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/ISPA.pdf.

ITU. "Question 17/13 – Packet forwarding and deep packet inspection for multiple services in packet-based networks and NGN environment." ITU website, last modified February 6, 2009. Accessed August 23, 2012. http://www.itu.int/ITU-T/studygroups/com13/sg13-q17.html.

Jaap-Koops, Bert. "Deep Packet Inspection and the Transparency of Citizens." In *Deep Packet Inspection: A Collection of Essays from Industry Experts*. Ottawa: Office of the Privacy Commissioner of Canada, 2009.

Jacobsen, Katherine. "Tech law blog Groklaw shuts down, cites surveillance concerns." *The Christian Science Monitor*, August 21, 2013. Accessed August 30, 2013.

http://www.csmonitor.com/Innovation/Responsible-Tech/2013/0821/Tech-law-blog-Groklaw-shuts-down-cites-surveillance-concerns.

Jones, Bryan D., and Frank R. Baumgartner. *The Politics of Attention: How Government Prioritizes Problem.* Chicago: The University of Chicago Press, 2005.

Kerr, Ian. "Online Service Providers, Fidelity, and the Duty of Loyalty." In *Ethics and Electronic Information*, edited by Thomas Mendina and Barbara Rockenbach. Jefferson, North Carolina: McFarland Press, 2002.

Kempf, J. and R. Austein (editors). "RFC 3724: The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture." *IETF*, March 2004. Accessed March 25, 2013. http://www.ietf.org/rfc/rfc3724.txt.

Kingdon, John W. *Agendas, Alternatives, and Public Policies (Second Edition).* Toronto: Longman, 2003.

Kiss, Jemima. "ISPs sign up to targeted ads deal." *The Guardian*, February 14, 2008. Accessed May 10, 2013. http://www.guardian.co.uk/media/2008/feb/14/bt.virginmedia.

Kravets, David. "Net Neutrality Groups Challenge AT&T FaceTime Blocking." *Wired*, September 18, 2012. Accessed May 1, 2013. http://www.wired.com/threatlevel/2012/09/factime-fcc-flap/.

Juniper Networks, Inc. "Call for Comments Response – Telecom Public Notice CRTC 2008-19." *CRTC*, February 19, 2009. Accessed March 23, 2012. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029277.DOC.

Kuhn, Andreas and Milton Mueller. "Profiling the Profilers: Deep Packet Inspection for Behavioural Advertising in Europe and the United States." *SSRN*, September 1, 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181.

La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression." United Nations Human Rights Council Twenty-third session, agenda item 3, April 17, 2013. Accessed August 30, 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Landau, Susan. *Surveillance or Security: The Risks Posed by New Wiretapping Technologies.* Cambridge, Mass.: The MIT Press, 2011.

Laser, Mathew. "FCC Order scolds Comcast for changing story on P2P blocking." *Ars Technica*, August 20, 2008. Accessed January 30, 2013. http://arstechnica.com/uncategorized/2008/08/fcc-order-scolds-comcast-for-changing-story-on-p2p-blocking/.

Langlois, S. Lerman. "Net Neutrality and Deep Packet Inspection: Discourse and Practice." In *Deep Packet Inspection: A Collection of Essays from Industry Experts.* Ottawa: Office of the Privacy Commissioner of Canada, 2009.

Lee, Dave. "Court orders UK ISPs to block more piracy sites." *BBC News*, February 28, 2013. Accessed May 12, 2013. http://www.bbc.co.uk/news/technology-21601609.

Lee, Timothy B. "ISP flip-flops: why do they now support "six strikes" plan?" *Ars Technica*, July 10, 2011. Accessed March 4, 2013. http://arstechnica.com/tech-policy/2011/07/why-did-telcos-flip-flop-and-support-six-strikes-plan/.

Lee, Timothy B. "Verizon: net neutrality violates our free speech rights," *Ars Technica*. July 3, 2012. Accessed June 13, 2013. http://arstechnica.com/tech-policy/2012/07/verizon-net-neutrality-violates-our-free-speech-rights/.

Lee, Timothy B. "Verizon called hypocritical for equating net neutrality to censorship." *Ars Technica*. November 16, 2012. Accessed May 15, 2013. http://arstechnica.com/tech-policy/2012/11/verizon-called-hypocritical-for-equating-net-neutrality-to-censorship/.

Lessig, Lawrence. *Code: Version 2.0.* New York: Basic Books, 2006.

Lichtbau, Eric. *Bush's Law: The Remaking of American Justice.* New York: First Anchor Books Edition, 2009.

Lo, Janet. "A "Do Not Track List" for Canada?" *Public Interest Advocacy Clinic*, October 2009. Accessed March 22, 2013. http://www.piac.ca/files/dntl_final_website.pdf.

The London School of Economic and Political Science. "Briefing on the Interception Modernisation Programme," *LSE,* 2009. Accessed November 10, 2012. http://www.statewatch.org/news/2009/jun/uk-lse-briefing-state-interception-prog.pdf.

Longford, Graham, Marita Moll, and Leslie Regan Shade. "From the "Right to Communicate" to "Consumer Right of Access": Telecom Policy Visions from 1970-2007." In *For $ale to the Highest Bidder: Telecom Policy in Canada*, edited by Marita Moll and Leslie Regan Shade. Ottawa: Canadian Centre for Policy Alternatives, 2008.

Lyon, David. *Surveillance Studies: An Overview.* Cambridge, UK: Polity, 2007.

Lyon, David. "Surveillance as social sorting: Computer codes and mobile bodies." In *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, edited by David Lyon. New York: Routledge, 2003.

McCullagh, Declan. "Senators call for end to Justice Department's 'secret law'." *CNet*, June 11, 2013. Accessed August 13, 2013. http://news.cnet.com/8301-13578_3-57588763-38/senators-call-for-end-to-justice-departments-secret-law/.

McManus, Mary. "Letter from Mary McManus, Senior Director of FCC and Regulatory Policy, Comcast Corporation, to Kris A. Monteith, Chief, Enforcement Bureau." *FCC*, File No. EB-08-IH-1518, at 5 (Jan. 25, 2008) (Comcast Response Letter).

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies and James Ball. "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013. Accessed June 21, 2013. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books, 2012.

Markey, Ed. "Key Lawmakers Question Local Provider Over Use of NebuAd Software Without Directly Notifying Customers," *House.gov*, July 14, 2008. Accessed February 6, 2013. http://markey.house.gov/press-release/july-15-2008-markey-embarq.

Markey, Edward J. and Joe Barton. "May 16, 2008 - Markey, Barton Raise Privacy Concerns About Charter Comm.," *House.gov*, May 15, 2008. Accessed February 6, 2013. http://markey.house.gov/press-release/may-16-2008-markey-barton-raise-privacy-concerns-about-charter-comm.

Marx, Gary. "Ethics for the New Surveillance." In *Visions of Privacy: Policy Choices for the Digital Age*, edited by Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press, 1999.

Masnick, Mike. "RIAA Admits It Wants DMCA Overhaul; Blames Judges For 'Wrong' Interpretation," *Techdirt*, November 8, 2011. Accessed May 15, 2013. https://www.techdirt.com/articles/20111108/00352916675/riaa-admits-it-wants-dmca-overhaul-blames-judges-wrong-interpretation.shtml.

Masnick, Mike. "NJ Gubenatorial Candidate Speaks Out Against Six Strikes: ISP Shouldn't Decide What You Can Download," *TechDirt*, February 25, 2013. Accessed March 4, 2013. https://www.techdirt.com/articles/20130225/10340922100/nj-gubenatorial-candidate-speaks-out-against-six-strikes-isp-shouldnt-decide-what-you-can-download.shtml.

Masnick, Mike. "PROTECT IP Renamed E-PARASITES Act; Would create The Great Firewall Of America," *Techdirt*, October 26, 2011. Accessed May 15, 2013. https://www.techdirt.com/articles/20111026/12130616523/protect-ip-renamed-e-parasite-act-would-create-great-firewall-america.shtml.

Meijerink, Sander V. "Understanding policy stability and change: The interplay of advocacy coalitions and epistemic communities, windows of opportunity, and Dutch coastal flooding policy 1945-2003." *Journal of European Public Policy* 12(6) (2005): 1060-1077.

Millar, Jason. "Core Privacy: A Problem for Predictive Data Mining." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock. Toronto: Oxford University Press, 2009.

Mitchell, Dan. "Say Goodnight, Bandwidth Hog," *The New York Times*, April 14, 2007. Accessed May 16, 2013. http://www.nytimes.com/2007/04/14/technology/14online.html.

Mochalski, Klaus, Hendrik Schulze, and Frank Stummer. "Copyright Protection in the Internet (Whitepaper)," *ipoque*, 2009. Accessed March 22, 2013. http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-copyright-protection-internet.pdf.

Mollett, Richard. "Digital Economy Bill Weekly Update 11 March 2010," *Craphound*, March 12, 2010. Accessed May 13, 2013. http://craphound.com/BPDigitalEconomyBillweeklyminutes.pdf.

Moodine, Austin. "Virgin trials P2P deep packet snooping." *The Register*, January 21, 2010. Accessed November 11, 2012. http://www.theregister.co.uk/2010/01/21/virgin_begins_cview_trials/.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom.* New York: Public Affairs, 2011.

Morris Jr, .John B. "Injecting the Public Interest into Internet Standards." In *Opening Standards: The Global Politics of Interoperability*, edited by Laura DeNardis. Cambridge, Mass.: The MIT Press, 2001.

Mosco, Vincent. *The Digital Sublime: Myth, Power, and Cyberspace.* Cambridge, Mass.: The MIT Press, 2004.

Motion Picture Association. "Submission of comments by the Motion Picture Association (MPA) in response to the Discussion on Traffic Management and "net neutrality"." *Ofcom*, September 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/MPA.pdf.

Ms. Smith. "HOPE 9: Whistleblower Binney says the NSA has dossiers on nearly every US citizen." *Network World,* July 15, 2012. Accessed March 8, 2013. https://www.networkworld.com/community/blog/hope-9-whistleblower-binney-says-nsa-has-dossiers-nearly-every-us-citizen.

Mueller, Milton. *Networks and States: The Global Politics of Internet Governance.* Cambridge, Mass.: The MIT Press, 2010.

Mueller, Milton, Andreas Kuehn, and Stephanie Michelle Santoso. "Policing the Network: Using DPI for Copyright Enforcement." *Surveillance and Society* 9(4) (2012): 348-364.

Mueller, Milton. "ITU Phobia: Why WCIT Was Derailed." *Internet Governance Project*, December 18, 2012. Accessed September 8, 2013, http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

Mullin, Joe. "How ISPs will do 'six strikes': Throttled speeds, blocked sites." *Ars Technica*, November 16, 2012. Accessed May 15, 2013. http://arstechnica.com/tech-policy/2012/11/how-isps-will-do-six-strikes-throttled-speeds-blocked-sites/.

Nakashima, Ellen. "NebuAd Halts Plans For Web Tracking." *Washington Post*, September 4, 2008. Accessed February 7, 2013. http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html?hpid=sec-tech.

National Science Foundation. "NSF Poses Code of Networking Ethics." *Communications of the ACM 32(6)* (1989): 505-506.

Neate, Rupert. "Phorm chief labels critics 'serial agitators'." *The Telegraph*, April 28, 2009. Accessed May 9, 2013. http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/5232565/Phorm-chief-labels-critics-serial-agitators.html

NebuAd. "NebuAd Announces Privacy Council." *Business Wire*, November 5, 2007. Accessed February 5, 2013. http://www.businesswire.com/news/home/20071105005667/en/NebuAd-Announces-Privacy-Council.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford University Press, 2010.

Nowak, Peter. "Net neutrality bill hits House of Commons." *CBC News*, May 28, 2008. Accessed March 20, 2012. http://www.cbc.ca/news/technology/story/2008/05/28/tech-netbill.html.

Nowak, Peter. "NDP to introduce 'net neutrality' private member's bill." *CBC News*, May 27, 2008. Accessed April 7, 2011. http://www.cbc.ca/news/technology/story/2008/05/27/net-neutrality-ndp.html.

Nuechterlein, Jonathan E. and Philip J. Weiser. *Digital Crossroads: American Telecommunications Policy in the Internet Age.* Cambridge, Mass.: The MIT Press, 2005.

O_2. "Telefónica O2 (UK) Limited Response To: "Traffic Management And 'Net Neutrality'" A Discussion Document." *Ofcom*, issued 2010. Accessed November 19, 2012. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Telef_nica_O2_UK.pdf.

Oates, John. "UK.gov tells throttling petition: Choke on it." *The Register*, July 18, 2008. Accessed November 7, 2012. http://www.theregister.co.uk/2008/07/18/epetition_broadband/.

Oates, John. "Phorm protestors picket BT AGM." *The Register*, July 18, 2008. Accessed May 8, 2013. http://www.theregister.co.uk/2008/07/16/bt_phorm_protest/.

O'Donnell, Shawn. "Broadband Architectures, ISP Business Plans, and Open Access." In *Communications Policy in Transition: The Internet and Beyond*, editors Benjamin M. Compaine and Shane Greenstein. Cambridge, Mass.: The MIT Press, 2001.

Ofcom. "List of ISPs." *Ofcom*. Accessed November 8, 2012. http://stakeholders.Ofcom.org.uk/telecoms/codes-of-practice/broadband-speeds-cop/list-of-isps/

Ofcom. "Voluntary Code of Practice: Broadband Speeds." *Ofcom*, June 5, 2008. Accessed November 8, 2012. http://stakeholders.Ofcom.org.uk/binaries/telecoms/cop/bb/copbb.pdf.

Ofcom. "Communications Market Report 2012." *Ofcom*, July 18, 2012. Accessed November 8, 2012. http://stakeholders.Ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf.

OfCom. "Traffic Management and 'net neutrality': A Discussion Document." *OfCom*, June 24, 2012. Accessed November 18, 2012. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf.

Ofcom. ""Site Blocking" to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act." *Ofcom*, May 27, 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.

Ofcom. "New measures to protect online copyright and inform consumers," *Ofcom*, June 26, 2012. Accessed May 12, 2013. http://media.ofcom.org.uk/2012/06/26/new-measures-to-protect-online-copyright-and-inform-consumers/.

Ohm, Paul. "The Rise and Fall of Invasive ISP Surveillance," *University of Illinois Law Review* 2009 (5) (2009): 1417-1496.

Office of the Privacy Commissioner of Canada. "What is DPI?" *Office of the Privacy Commissioner of Canada*, April 2009.

Office of the Privacy Commissioner of Canada. "Policy Position on Online Behavioural Advertising," *Office of the Privacy Commissioner of Canada*, June 6, 2012. Accessed September 9, 2013. http://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp.

Office of the Privacy Commissioner of Canada. "PIPEDA Case Summary #2009-010 – Report on Findings: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection." *Office of the Privacy Commissioner of Canada,* September 2009. Accessed March 27, 2012. http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm.

Open Media. "Police Chiefs spend tax dollars to lobby for warrantless online surveillance." *OpenMedia,* January 18, 2012. Accessed June 22, 2012. http://openmedia.ca/news/police-chiefs-spend-tax-dollars-lobby-warrantless-online-surveillance.

Open Rights Group. "Ofcom Net Neutrality consultation." *Ofcom*, September 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/ORG.pdf.

Open Rights Group. "Communications Data Bill." *Open Rights Group*, updated May 10, 2013. Accessed May 12, 2013. http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill.

Open Rights Group. "Communications Capabilities Development Programme." *Open Rights Group*, May 5, 2013. accessed May 12, 2013. http://wiki.openrightsgroup.org/wiki/Communications_Capabilities_Development_Programme#EU_Law.

Orman, Hilarie. "The Morris Worm: A Fifteen-year Perspective," *Security and Privacy, IEEE* 1(5) (2003): 35-43.

Parsons, Christopher, Alexander Ly, Steve Anderson, and Shea Sinnott. "The Open Internet: Open for Business and Economic Growth." In *Casting and Open Net: A Leading-Edge Approach to Canada's Digital Future*, edited by Steve Anderson and Reilly Yeo. 2011.

Parsons, Christopher. "Rogers, Network Failures, and Third-Party Oversight." *Technology, Thoughts, and Trinkets*, December 2, 2010. Accessed June 20, 2012. http://www.christopher-parsons.com/blog/isps/rogers-network-failures-and-third-party-oversight/.

Parsons, Christopher. "Agenda Denial and UK Privacy Advocacy." *Technology, Thoughts, and Trinkets*, January 19, 2011. Accessed May 13, 2013. http://www.christopher-parsons.com/agenda-denial-and-uk-privacy-advocacy/.

Parsons, Christopher. "Aggregating Information About CView." *Technology, Thoughts, and Trinkets,* December 17, 2009. Accessed March 22, 2013. http://www.christopher-parsons.com/aggregating-information-about-cview/.

Parsons, Christopher. "Lawful Access is Dead; Long Live Lawful Intercept!" *Technology, Thoughts, and Trinkets*, February 11, 2013. Accessed April 9, 2013. http://www.christopher-parsons.com/lawful-access-is-dead-long-live-lawful-intercept/.

Pierson, Paul. "When Effect Becomes Cause: Policy Feedback and Policy Change." *World Politics* 45(1) (1993): 595-628.

Pierson, Paul. "Not Just What, But *When*, Timing and Sequence in Political Processes." *Studies in American Political Development* 14 (2000): 72-92.

PIAC. "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers – Comments of the Consumers' Association of Canada, the National Anti-Poverty Organization and the Option consommateurs ("The Consumer Groups")." *CRTC*, February 23, 2009. Accessed March 23, 2012. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030499.zip.

Policy Engagement Network. "Briefing on the Interception Modernisation Programme." *London School of Economics and Political Science,* 2009. http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf.

Pollach, Irene. "What's Wrong with Online Privacy Policies?" *Communications of the ACM* 50(9) (2007): 103-108.

Pool, Ithiel de Sola. *Technologies of Freedom*. Cambridge, Mass.: The Belknap Press of Harvard University Press, 1993.

Porter, Thomas. "The Perils of Deep Packet Inspection." *Symantec Corporation*, last modified October 19, 2010. Accessed March 21, 2013. http://www.symantec.com/connect/articles/perils-deep-packet-inspection

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

Her Majesty Queen Elizabeth II. "The Queen's Speech 2013." UK Parliament, May 8, 2013. Accessed May 13, 2013. https://www.gov.uk/government/speeches/the-queens-speech-2013.

RadiSys. "DPI: Deep packet inspection motivations, technology, and approached for improving broadband service provider ROI." *RadiSys* (2010). http://www.radisys.com/Documents/papers/DPI_WP_Final.pdf.

Rast, Joel. "Why History (Still) Matters: Time and Temporality in Urban Political Analysis," *Urban Affairs Review* 48(3) (2012): 3-36.

Reardon, Marguerite. "Comcast denies monkeying with BitTorrent traffic." *CNet*, August 21, 2007. Accessed May 15, 2013. http://news.cnet.com/8301-10784_3-9763901-7.html.

Reed, David P., Jerome H. Saltzer, and David D. Clark. "Active Networking and End-to-End Arguments." *IEEE Network* 12(3) (1998): 220-228.

Regan, Priscilla. *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press, 2002.

Reidenberg, Joel R. "Lex Informatica: The Formation of Information Policy Rules Through Technology." *Texas Law Review* 76(3) (1998): 553-584.

Rekhter, Yakov, Bruce Davie, Eric Rosen, George Swallow, Dino Farinacci, and Dave Katz. "Tag Switching Architecture Overview." *Proceedings of the IEEE* 82(12) (1997):1973-1983.

Renals, Peter, and Grant A. Jacoby. "Blocking Skype through Deep Packet Inspection." Paper presented at *42nd Hawaii International Conference on System Sciences,* Waikoloa, Big Island, Hawaii, January 5-8, 2009.

Reynolds, J.K. "RFC 1135: Helminthiasis of the Internet." *IETF Network Working Group* (1989). Accessed March 25, 2013. https://tools.ietf.org/html/rfc1135.

Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review* 126 (2013): 1934-1965.

Riley, M. Chris and Ben Scott. "Deep Packet Inspection: The end of the Internet as we know it?" *Freepress* (2009). Accessed: June 18, 2011. http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf.

Risen, James. *State of War: The Secret History of the CIA and the Bush Administration*. Toronto: Free Press, 2006.

Risen, James and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." *New York Times*, December 16, 2005. Accessed March 19, 2013. http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

Rogers. "Canadian Association of Internet Providers (CAIP) - Application requesting certain orders directing Bell Canada to cease and desist from throttling its wholesale ADSL Access Services." *CRTC,* July 3, 2008. Accessed March 21, 2012. http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923478.pdf.

Rogers. "Telecom Public Notice CRTC 2008-19 – Review of Internet traffic management practices of Internet service provider – Rogers Reply Comments." *CRTC*, April 30, 2009. Accessed June 28, 2009. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/111039 2.pdf.

Rosen, Eric, and Yakov Rekhter. "RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNS)." *IETF* (2006). Accessed June 25, 2011. http://tools.ietf.org/html/rfc4364.

Saltzer, J. H., D. P. Reed, and D. D. Clark. "End-to-End Arguments in System Design." *ACM Transactions on Computer Systems* 2(4) (1984): 277-288.

Sandoval, Greg. "Sources: AT&T, Comcast may help RIAA foil piracy." *CNet*, January 28, 2009. Accessed March 8, 2013. http://news.cnet.com/8301-1023_3-10151389-93.html.

Savage, Charlie. "Senators Say Patriot Act Is Being Misinterpreted." *The New York Times,* May 26, 2011. Accessed August 9, 2013. http://www.nytimes.com/2011/05/27/us/27patriot.html.

Schmidt, Susan K., and Raymund Werle. *Coordinating Technology: Studies in International Standardization of Telecommunications.* Cambridge, Mass.: The MIT Press, 1998.

Schneider, Anne and Helen Ingram. "Social Construction of Target Populations: Implications for Politics and Policy." *The American Political Science Review* 87(2) (1995): 334-347.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security In An Uncertain World.* United States: Springer, 2006.

Schoen, Seth. "Detecting Packet Injection: A guide to observing packet spoofing by ISPs." *Electronic Frontier Foundation*, November 28, 2007. Accessed March 22, 2013. https://www.eff.org/files/packet_injection.pdf.

Scorrock, Tim. *Spies for Hire: The Secret World of Intelligence Outsourcing.* Toronto: Simon & Schuster Paperbacks, 2008.

Shade, Leslie Regan. "Public Interest Activism in Canadian ICT Policy: Blowin' in the Policy Winds." *Global Media Journal: Canadian Edition 1(1)* (2008): 107-121.

Shaw, "Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers – Reply Comments," *CRTC*, April 30, 2009, accessed June 28, 2009, http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/110988 5.pdf.

Shelton, Dominique R. and Stephanie Quick. "Online behavioral advertising – summary of Senate Commerce Committee hearing on July 9, 2008 concerning privacy implications of behavioral ad targeting." *Edwards Wildman Palmer LLP*, July 14, 2008. Accessed March 4, 2013. http://www.lexology.com/library/detail.aspx?g=7ca7187a-56e2-4224-bd31-46ed7f2d1540.

Skype. "Before the Canadian Radio-television and Telecommunications Commission In the Matter of an Application by Canadian Association of Internet Providers Pursuant to Part VII of the CRTC Telecommunications Rules of Procedure and Sections 7, 24, 25, 32, 36 and 62 of the *Telecommunications Act* Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" Its Wholesale ADSL Access Services." *CRTC*,

June 12, 2008. Accessed October 3, 2012. http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/920240.PDF.

Singel, Ryan. "New Facebook Messaging Continues to Block Some Links." Wired, November 18, 2010. Accessed September 9, 2013. http://www.wired.com/business/2010/11/facebook-link-blocking/.

Smith, Ashiya N. "NebuAd Introduces Next-Generation Online Consumer Privacy Protections, Raising the Bar on Internet Privacy Protection Standards." *Business Wire*, July 8, 2008. Accessed May 17, 2013. http://www.businesswire.com/news/home/20080708005383/en/NebuAd-Introduces-Next-Generation-Online-Consumer-Privacy-Protections.

Smouts, Marie-Claude. "The proper use of governance in international relations." *International Social Science Journal* 50(155) (1998): 81-89.

Sohn, David. "Content Filtering Kept Out of Broadband Stimulus, At Least for Now." *Centre for Democracy & Technology*, February 11, 2009. Accessed May 11, 2013. https://www.cdt.org/blogs/david-sohn/content-filtering-kept-out-broadband-stimulus-least-now.

Solon, Olivia. "Tim Berners-Lee: deep packet inspection a 'really serious' privacy breach." *Wired UK*, April 18, 2012. Accessed May 7, 2013. http://www.wired.co.uk/news/archive/2012-04/18/tim-berners-lee-dpi/viewgallery/283287.

Solove, Daniel. *The Digital Person: Technology and Privacy in the Information Age.* New York: New York University Press, 2004.

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

Sonicwall. "10 Cool Things Your Firewall Should Do." *Sonicwall*, 2008. Accessed February 3, 2013. http://www.sosonicwall.com/lib/deciding-what-solution/10_Things_Your_Firewall_Should_Do.pdf.

Sourdis, Ioannis. *Designs & Algorithms for Packet and Content Inspection.* Delft: TU. Delft, 2007.

Stoddart, Jennifer. "Commissioner's introduction to DPI research volume." In *Deep Packet Inspection: A Collection of Essays from Industry Experts*. Office of the Privacy Commissioner of Canada, April 2009.

Steeves, Valerie. "Reclaiming the Social Value of Privacy." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock. Toronto: Oxford University Press, 2009.

Sunstein, Cass. *Republic.com.* Princeton, New Jersey: Princeton University Press, 2001.

Svensson, Peter. "Comcast blocks some Internet traffic." *Associated Press*, October 19, 2007. Accessed May 17, 2013. http://www.nbcnews.com/id/21376597/.

TELUS. "Part VII application by Canadian Association of Internet Providers (CAIP) requesting that the Commission issue certain orders directing Bell Canada to cease and desist from "throttling" wholesale ADSL services and in particular, the wholesale service known as Gateway Access Service (GAS)." *CRTC*, July 3, 2008. Accessed March 24, 2012. http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153_1/923480.pdf.

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

Topolski, Robb ("Funchords"). "Comcast is using Sandvine to manage P2P Connections." *DSL Reports Forum*, May 12, 2007. Accessed September 7, 2013. http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections.

Topolski, Robert M. "NebuAd and Partner ISPs: Wiretapping, Forgery, and Browser Hijacking." *Free Press* and *Public Knowledge*, June 18, 2008. Accessed March 22, 2013. http://www.freepress.net/files/NebuAd_Report.pdf.

Travis, Alan. "Queen's speech revives 'snooper's charter' legislation." *The Guardian*, May 8, 2013. Accessed May 13, 2013. http://www.guardian.co.uk/politics/2013/may/08/queens-speech-snoopers-charter.

Travis, Alan, Patrick Wintour, and Haroon Siddique. "'Snooper's charter': Clegg kills of Tory hopes of deal on rewritten plan." *The Guardian*, April 26, 2013. Accessed May 13, 2013. http://www.guardian.co.uk/world/2013/apr/25/snoopers-charter-nick-clegg-agreement.

Turkle, Sherry. *Alone Together: Why we expect more from technology and less from each other*. New York: Basic Books: 2011.

Turow, Joseph. "Americans and Online Privacy: The System is Broken (research report)." The Annenberg Public Policy Center of the University of Pennsylvania, June 2003. Accessed September 7, 2013. http://www.ftc.gov/bcp/workshops/infoflows/comments/030618turow.pdf.

UK Government. "Regulation of Investigatory Powers Act," *Legislation.gov.uk*, 2000 c. 23. Accessed June 4, 2013. http://www.legislation.gov.uk/ukpga/2000/23/contents.

UK Parliament. "Daily Hansard – Written Answers," *www.parliament.uk*, November 19, 2008. Accessed May 12, 2013. http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm081119/text/81119w0032.htm#08112012001081.

United States Government Accountability Office. "Intellectual Property: Observations on Effects to Quantify the Economic Effects of Counterfeit and Pirated Goods." United States Government, 2010.

Utech, Anne. "Ubiquitous Computing and Spatial Privacy." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock. Toronto: Oxford University Press, 2009.

van Schewick, Barbara. *Internet Architecture and Innovation.* Cambridge, Mass.: The MIT Press, 2010.

Vibber, Brion. "Wikimedia Foundation opting out of Phorm." *Wikimedia Blog*, April 16, 2009. Accessed May 10, 2012. https://blog.wikimedia.org/2009/04/16/wikimedia-opting-out-of-phorm/.

Vaxination Infomatique. "Re: Public Telecom Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet Service Providers – Reference: 8646-C12-200815400." *CRTC*, February 23, 2009. Accessed March 21, 2012. http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029877.pdf.

Vincent, Charles and Jean Camp. "Looking to the Internet for models of governance." *Ethics and Information Technology* 6 (2004): 161-173.

Vodafone. "Traffic Management and 'net neutrality'." *Ofcom*, September 2010. Accessed November 19, 2012. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Vodafone.pdf.

Vuze. "Bad ISPs." *Vuze* Wiki, modified as of October 12, 2012. Accessed November 8, 2012. http://wiki.vuze.com/w/Bad_ISPs#United_Kingdom.

Waters, Darren. "Amazon blocks Phorm adverts scan." *BBC News*, April 15, 2009. Accessed May 10, 2013. http://news.bbc.co.uk/2/hi/technology/7999635.stm.

Waters, Darren. "Home Office 'colluded with Phorm'." *BBC News*, April 28, 2009. Accessed May 10, 2013. http://news.bbc.co.uk/2/hi/technology/8021661.stm.

Waters, Darren. "Phorm hoping to stop 'phoul play'." *BBC News*, April 28, 2009. Accessed May 10, 2013. http://www.bbc.co.uk/blogs/technology/2009/04/phorm_hoping_to_stop_phoul_pla.html.

Williams, Christopher. "Police quiz BT on secret Phorm trials." *The Register*, September 5, 2008. Accessed May 9, 2013. http://www.theregister.co.uk/2008/09/05/bt_phorm_police_meeting/.

Williams, Christopher. "Home Office defends 'dangerously misleading' Phorm thumbs-up." *The Register*, April 24, 2012. Accessed November 10, 2012. http://www.theregister.co.uk/2008/04/24/home_office_phorm_fipr_bt/.

Williams, Christopher. "UK.gov to spend £2bn on ISP tracking." *The Register*, April 27, 2009. Accessed November 29, 2012. http://www.theregister.co.uk/2009/04/27/imp_consultation/.

Williams, Christopher. "Virgin Media mops up CEO's 'boll*cks' outburst." *The Register*, April 15, 2008. Accessed November 8, 2012. http://www.theregister.co.uk/2008/04/15/virgin_media_net_neutrality/.

Williams, Christopher. "Virgin Media rubbishes P2P throttling rumours." *The Register*, June 23, 2008. Accessed November 8, 2012. http://www.theregister.co.uk/2008/06/23/virgin_media_application_throttling_denial/.

Williams, Christopher. "Virgin Media to dump neutrality and target BitTorrent users." *The Register*, December 15, 2008. Accessed November 8, 2012. http://www.theregister.co.uk/2008/12/16/virgin_bittorrent/.

Williams, Christopher. "Virgin Media distances itself from Phorm 'adoption' claims." *The Register*, May 1, 2008. Accessed May 10, 2013. http://www.theregister.co.uk/2008/05/01/virgin_media_phorm_misleading/.

Williams, Christopher. "FIPR: ICO gives BT 'green light for law breaking' with Phorm." *The Register*, April 8, 2008. Accessed May 2, 2013. http://www.theregister.co.uk/2008/04/07/bt_phorm_ico/.

Williams, Christopher. "Mobile networks line up to bash net snooping plan." *The Register*, December 22, 2009. Accessed May 13, 2013. http://www.theregister.co.uk/2009/12/22/mobile_imp/.

Williams, Christopher. "EU threatens 'formal action' against UK.gov on Phorm." *The Register*, February 11, 2009. Accessed May 2, 2013. http://www.theregister.co.uk/2009/02/11/phorm_eu_action_threat/.

Winner, Langdon. *The Whale and the Reactor.* Chicago: The University of Chicago Press, 1986.

Wolfson, Stephen Manuel. "The NSA, AT&T, and the Secrets of Room 641A." *I/S – A Journal of Law and Policy for the Information Society* 3(3) (2007): 411-441.

World Wide Web Consortium. "Privacy Activity" W3C website. Accessed March 25, 2013. http://www.w3.org/Privacy/.

World Wide Web Consortium. "Help and FAQ >> What Does W3C Do?" *W3C*. Accessed March 25, 2013. http://www.w3.org/Help/#activity.

Yahoo! UK & Ireland. "Traffic management and 'net neutrality': A discussion document." *Ofcom*, September 2010. Accessed May 12, 2013. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/responses/Yahoo.pdf.

Young, Iris Marion. "Activist Challenges to Deliberative Democracy." *Political Theory* 29:5 (2001): 670-690.

Zachem, Kathryn A. "Letter from Kathryn A. Zachem, Vice President of Regulatory Affairs, Comcast Corporation, to Marlene H. Dortch, Secretary," *FCC*, at 5 (July 10, 2008) (Comcast Technical Ex Parte).

Zalewski, Michael. *Silence on the Wire: a Field Guide to Passive Reconnaissance and Indirect Attacks.* San Francisco: No Starch Press, 2005.

Zetter, Kim. "Former NSA Official Disputes Claims by NSA Chief." *Wired*, July 29, 2013. Accessed March 3, 2013. http://www.wired.com/threatlevel/2012/07/binney-on-alexander-and-nsa/.

Zittrain, Jonathan. *The Future of the Internet – And How To Stop It.* New Haven: Yale University Press, 2008.