© 2010, *Global Media Journal -- Canadian Edition* Volume 3, Issue 1, pp. 51-73
ISSN: 1918-5901 (English) -- ISSN: 1918-591X (Français)

# Ends and Ways:

# The Algorithmic Politics of Network Neutrality *

*Fenwick McKelvey*

Ryerson University, Canada

***Abstract:***

The Internet in Canada is an assemblage of private and public networks. A variety of institutions and networking codes manage these networks. Conflicts exist between these parties despite their interconnection. Tensions heightened when commercial ISPs began managing traffic on their network using sophisticated routing algorithms. Concerned parties demanded legislation based on a network neutrality principle to prevent undue discrimination. While the network neutrality controversy has been addressed as a question of public policy, the controversy also includes a conflict between various codes constituting networks in Canada. The conflict between codes involve two key networking software that manifest incongruous networks. Their algorithms, the logics embedded in code, differentiate the different types of networking code. The two types of algorithms are Quality of Service and End-to-End. These algorithms treat different modalities of Internet communication differently, in part due to their deployment by different institutions. Quality of Service allows for the tiering of traffic by carriers. Commercial carriers have popularized this algorithm to promote value-added services and prevent network congestions. End-to-end algorithms, on the other hand, enforce a strict equality between modalities of communication. Peer-to-peer applications have popularized an extreme version of the end-to-algorithm, treating all nodes as equals. The popularity and growth of both these algorithms pulls the Internet in different directions, creating conflicts over its future. Through an extended review of these two algorithms and their intersection, this paper confronts how code plays a role in the network neutrality controversy.

***Keywords:*** Telecommunications; Public Interest; Networking; Discrimination; Algorithms

***Résumé:***

Internet au Canada est un assemblage de réseaux privés et publics. Un grand nombre d'institutions et de codes de réseautage régissent ses réseaux. Des conflits existent entre ces parties au mépris de leur interconnexion. Cette tension a augmenté quand les fournisseurs de services Internet ont commencé à gérer le trafic sur leurs réseaux en utilisant des algorithmes de routage sophistiqués. Des parties soucieuses ont demandé la création de la législation basée sur le principe de la neutralité du réseau afin d'éviter une discrimination injustifiée. Autant que la controverse entourant la neutralité a été adressée comme une question de politiques publique, la controverse enferme aussi un conflit entre plusieurs codes qui forment un réseau au Canada. Le conflit entre des codes de réseautage concerne deux codes de réseautage clefs qui démarquent des réseaux disparates. Leurs algorithmes, la logique qui est contenue dans les codes, sont ce qui différencie les différents types de code de réseautage. Les deux types d'algorithmes sont *la qualité du service* et *de bout en bout*. Ces algorithmes traitent les modalités de la communication par Internet différemment, occasionnés en partie par leur déploiement par des institutions différentes. La qualité du service permet l'étagement du trafic par les fournisseurs. Les fournisseurs commerciaux ont popularisé cet algorithme afin de promouvoir des services à valeur ajoutée et pour empêcher l'engorgement des réseaux. Cependant, les algorithmes de bout en bout appliquent une égalité rigoureuse entre les modalités de communication. Des applications poste-à-poste ont rendu populaire une version extrême de la fin de l'algorithme, en traitant tous les nœuds en égales. La popularité et la croissance de ces deux algorithmes tirent l'Internet dans deux directions différentes et créent des conflits à propos de son future. À travers une revue exhaustive de ces deux algorithmes et de leur intersection, cet article affronte la façon dont les codes jouent un rôle dans le débat entourant la neutralité du réseau.

***Mots-clés:*** Télécommunications; Intérêt public; Réseautage; Discrimination; Algorithmes

---

## Introduction

Divergent processes of networking compete to shape the Internet in Canada. The competition occurs between the few major Internet service providers (ISPs), and, importantly, between the software networking the Internet together. Software running on home computers competes with software running on network routers to shape how information moves across the Internet. Bell Canada's Internet service exemplified this competition when it installed software on its networks to slow home peer-to-peer traffic, while launching its own premium services to sell ringtones,

movies, and music[1] (Kapica, 2008). This example fits into an emerging trend among ISPs to use traffic management software to streamline their networks, prevent congestion, and promote value-added services. The trend has sparked a public controversy over the regulation of the Internet. Public backlash to the ISPs' direction has demanded *network neutrality legislation* that mandates networks to treat all communication equally in order to protect the Internet as a public medium and to prevent carriers from discriminating against traffic for commercial gain. Where policy actors have debated network neutrality under the auspices of the Canadian Radio-television and Telecommunications Commission (CRTC 2008; 2009b), the conflict also involves different networking software that has yet to receive proper representation. Software is a part of the controversy not wholly expressed by the different parties in policy circles since it has its own politics beyond its political expression (Barney, 2000; Galloway, 2004; Karaganis, 2007; Latham & Sassen, 2005b; Lessig, 2006).

The following paper contributes an analytic for the politics of networking software and employs this analytic to represent the software involved in the network neutrality controversy. The analytic involves the concept of networking, the logics of networks, and the logics embedded in software, known as algorithms. Network neutrality, then, involves a conflict between classes of algorithms with particular logics that constitute two competing processes of networking**.** These two competing processes of networking are end-to-end (E2E) and quality of service (QoS). The core of the paper investigates the network relations and algorithms that constitute E2E and QoS networking. The emphasis on algorithms contributes towards a software studies approach (Chun, 2005; Fuller, 2003, 2008b; Manovich, 2002) to understand how networking operates and to link network neutrality with an emerging research in algorithms as a mechanism of political control (Beer, 2009; Galloway, 2006; Graham, 2005; Lash, 2007). The analytics, in sum, fills a gap by providing a language to discuss the competing processes of networking and by revealing their political significance to the network neutrality controversy.

The paper begins by distinguishing a software studies approach from the literature on the sociology and technology of networks. Software studies compliments this literature by adding a sense of the political components of the technologies involved with Internet cultures. Software studies, however, have only begun to investigate networking software. As a contribution, the following section introduces an analytic for the study of networking software. Networks, algorithms, and logics emerge as central concepts in the study of the political dimension of networking (Fuller, 2008b; Graham, 2005; Lash, 2007; Latham, 2005). The terms provide the means to investigate the algorithms involved in the network neutrality controversy. Beginning with end-to-end algorithms and moving to Quality of Service algorithms, the paper discusses their logics, deployments, and operations. The sections explicate the two competing processes of networking that will then be discussed in the conclusion in relation to network neutrality. These observations contribute toward a more robust explanation of network neutrality—one that gives the technical side proper representation.

## Literature Review

Proponents and critics of network neutrality have created a growing literature debating the legislation. Since the perspectives have already been covered in depth[2], this section will not duplicate an exhaustive overview; rather, it will characterize a few positions to present a sense of the politics of the controversy. Network neutrality advocates demand packet equality where "all packets transmitted over the public Internet be treated equally, regardless of source, ownership,

content, or destination" (Longford, 2007: 13). The principle, advocates suggest, would prevent the discrimination of traffic. Anti-discrimination means that "those who own the networks do not also control the content that runs over them" (Moll & Shade, 2008: 407). Communication networks, as Moll and Shade believe, should serve the public interest, not just its shareholders. Critics of a network neutrality principle, on the other hand, suggest discrimination would allow commercial Internet service providers to remain competitive by tailoring their product to consumer needs. Networks are a service delivered for a profit and managing traffic aids in profitability (Wu & Yoo, 2007; Yoo, 2004).

These statements reveal the underlying political component of the controversy: a clash over the "normative concept of what communication is supposed to do" (Sandvig, 2007: 145). The network neutrality controversy involves deep-seated political cleavages over the purpose of communication networks. Should all packets be treated the same or should some be marginalized? A variety of answers emerge to the questions of "how Internet infrastructure is built, who pays for it, and who benefits from it" (Barratt & Shade, 2007: 295). Different understandings of the web justify political claims, politicizations of technology, and the treatment of packets. In other words, "that how 'the Internet' is understood has substantial legal, social, and cultural consequences" (Crawford, 2007: 467). Thus, the controversy involves the collision of different perspectives toward the Internet.

Political cleavages about the Internet have often been framed as a collision between different socio-technical cultures. Frieden argued that the "technological and marketplace convergence has triggered a clash of cultural identities and regulatory philosophies" (2002: 426). Frieden introduced a socio-technical approach to the clash when he described the two main factions: Netheads (Internet libertarians), and Bellheads (telecommunication executives). Crawford (2007) expanded his list to include engineers, Telcos, and Netheads who compete to define the Internet. Engineers refer to those involved in the technical construction of the Internet beginning in the 1970s. The Telco perspective comes from the history of telephony and sees the Internet as another commodity service. Finally, the Nethead perspective sees the Internet as a social good—a way to augment human understanding and cooperation (Crawford, 2007). Network neutrality, from a socio-technical approach, concerns the different ways each of these groups comprehend and stabilize[3] their understanding of the Internet. Telcos might see network neutrality as a problem of pricing, engineers might see it as a technical issue, and Netheads might see it as a battle over Internet freedom.

Software plays a key role in the politics of Internet cultures. Netheads, engineers, and telcos derive their views, in part, from their interpretation of the software running online. Gillespie (2006) argues that the E2E principle inspired generations of advocates of Internet free speech. Nethead John Perry Barlow, for example, once famously quipped, "the Internet treats censorship as a malfunction and routes around it". Different factions then circulate their interpretations of the Internet's code as an objective definition[4] that justifies their position. "There is a neat discursive fit between the populist political arrangements [Barlow] seeks", Gillespie points out, "and the technical design of the network that he believes hands users power" (2006: 443). The example of Barlow illustrates the translation of code into politics.

Cultures not only understand the Internet, they also write software to re-produce their understandings. Netheads, such as free software developers, write software that reproduces their view of equality for all packets. Internet cultures often re-produce their politics into software that, in turn, comes to life. Software aids the spread of their political vision because of the "manipulative capacities engendered by digital technologies" (Latham & Sassen, 2005a: 17).

The manipulative capacity of software entails how it *controls* input through "purposive influence toward a predetermined goal" (1986: 7). Software, in short, acts politically when it gently guides the informational flows of the Internet. The network neutrality controversy, then, needs to understand how the software is produced and operating online, not just the associated Internet cultures.

A literature has emerged addressing the politics of code. Lawrence Lessig famously explained the politics of code as comparable to law. He argued for the need to understand "how the software and hardware (i.e., the 'code') that make cyberspace what it is also regulates cyberspace as it is" (2006: 5). To his calls and others, the emerging field of software studies (Fuller, 2008b) attempts to explicate the ramifications of software:

> [R]ather than simply watch and make notes on the humans lit by the glow of their monitors, it [software studies] aims to map a rich seam of conjunctions in which the speed and rationality, or slowness and irrationality, of computation meets its ostensible outside (users, culture, aesthetics) but is not epistemically subordinated by it.
>
> (Fuller, 2008a)

Software becomes a central concept to analyze the politics of code, yet even the category of software remains too broad. Most studies in response have focused on specific types of software, such as the software involved in the formation of the Internet.

Much of the software studies research on the Internet focuses on the role of software in mediating the user experience, such as search engines (Halavais, 2009; Introna & Nissenbaum, 2000), web platforms (Burgess & Green, 2009; Langlois, McKelvey, Elmer, & Werbin, 2009; Mackenzie, 2006; van Dijck, 2009), and desktop software to connect online (Elmer, 2002; Ripeanu, Mowbray, Andrade, & Lima, 2006). Explicit studies of actual networking software remain largely absent in the literature. The closest theme has been the study of *protocols* (DeNardis, 2009; Elmer, 2008; Galloway, 2004). Protocols "are all the conventional rules and standards that govern relationships within networks" (Galloway & Thacker, 2004: 8). Problematically, the protocol frames network formation as the product of homogeneous pacts written by computer programmers and policy makers, such as the Internet Protocol Suite (TCP/IP). The network neutrality controversy, despite the prominence of the TCP/IP, thwarts a simple causality between protocols and networks. The network is not a unified form resulting from protocols, but rather conflicting processes of networking enabled by software. The following section, then, proposes an analytic to study algorithms and their processes of networking.

**Networking: Network Relations, Processors, and Algorithms**

Suggesting algorithms as a concept to study networking may seem problematic because "selecting singular examples from the World Wide Web in order to support claims about the Web… is a lot like manufacturing one's own evidence, minting one's own coin" (Gitelman, 2006: 130). Why not rely on an established concept, such as protocols? Algorithms capture the *activity* of networks. The software component animates broadband pipes, and, while protocols do capture vital aspects of the Internet, the picture would not be complete without putting software under the microscope to reveals its specific, one might say microbial, cultures. Perhaps the best

way to consider the utility of the algorithm will come from beginning with the question of what is the Internet, questioning its formation, and then focusing on the logics and processes enacting this formation. The algorithm then appears as a key concept in the answer to these questions.

The Internet is a process of internetworking private and public networks using the Internet Protocol Suite. The common protocols guide the construction and transportation of information using a packet-switching method. Software assembles, routes, and disassembles information online as small discrete bits of information, known as packets. All nodes of the network use the same protocol for packet switching, thereby allowing their interconnection. While the method to use computers and packets to transmit information evolved in the 1950s in the United States and England, actually creating a global network using packet switching took nearly fifty more years of development. Packet switching gradually arose as a viable alternative to the conventional *circuits* telecommunication systems of the time. Packet switching did not become an alternative until the release of TCP/IP in the 1970s and 1980s[5] by the Advanced Research Projects Agency (ARPA). Gradually, TCP/IP became the standard protocol for computer networks as its adoption spread beyond the United States and the rest of the world (Abbate, 1999; Gillespie, 2006).

TCP/IP, throughout its spread, faced steep competition from other processes of internetworking, such as the Open Systems Interconnection (OSI) model (Latham, 2005). The question arises: how did its processes of networking succeed or, to put it another way, "why does an internetwork comprising such varying network types and scales come into being to become the primary global computer communication system" (Latham, 2005: 148). Latham suggests the answer lies in the logics "whereby computer networks would form and then connect or not connect (and the consequences of such formation and connection)" (2005: 149). He refers to these logics as the relations among networks, or what will be called *network relations*. Network relations emphasize how networking *is a process, not a shape*. Network relations connect networks together and also rationalize interconnection to the owners and administrators. Latham points out how the Internet's ad-hoc network relations eclipsed the OSI model of network because of its ease to deploy without major network re-configuration. While Latham's argument about the TCP/IP and OSI cannot be summarized in full here, the example demonstrates how networking has particular logics of connection. Crucially, the processes of networking involve compromises and limitations, not only the creation of larger networks. Although the merits of the OSI model remain debatable, its formulation attempted to respond to concerns about how to track the carriage of information and charge for the cost.

Network relations become part of the software that connects networks and constitutes the Internet. As Sassen writes, the Internet is "a space produced and marked through the software that gives it its features and the particular aspects of the hardware mobilized by the software" (Sassen, 2000: 20). Software resides on computer desktops and on routers, called network processors, running in networks owned by Internet Service Providers (Lekkas, 2003). Focusing on software enables a comparison of these various layers of Internet and the diversity of software running online.

Network relations embed in software as *algorithms*. Goffey defined the algorithm as the combination of logic (network relations) and control (code). He states, "algorithms do things and their syntax embodies a command structure to enable this to happen" (Goffey, 2008: 17). In effect, algorithms become a way to enact the logics of network relations which become the "goals toward which a process is to be influenced and the procedures for processing additional information toward that end" (Beniger, 1986: 40). Algorithms treat packets as input that its

logics or network relation interpret and act upon—usually sending a packet closer to its destination. The operations of algorithms and their interactions create processes of networking. The multiplicity of algorithms implies a multiplicity of network forms, all joining, separating, colliding, and converging online.

Algorithms have a politics because they distribute and utilize finite network resources to transmit packets. Transmission differs in how algorithms might prioritize some packets to ensure their fast and lossless delivery at the expense of other packet that must receive fewer resources. Their politics, in turn, define the ensuing processes of networking (Graham, 2005). Do algorithms treat packets equally? Home computers might use peer-to-peer algorithms to share files, while servers could use queuing algorithms to mange bandwidth, and routers may employ quality of service algorithms to prioritize packets. Comparing algorithms entails considering the different ways they process packets according to their encoded network relations. How algorithms process packets, in other words, defines its networking processes. The analytic then questions how algorithms process packets according to their network relations and how their processes enact specific processes of networking.

If algorithms enable networking, then the state of the Internet might be best explained through a discussion of the dominant algorithms online. What algorithms might be involved in generating its form? Since multiple algorithms exist online, the Internet is woven from the undulating threads of distinct and competing algorithms. As previously introduced, end-to-end algorithms and quality of service algorithms underlie much of the core controversy in network neutrality. In the following sections, these two types of algorithms will be explored to reveal their network relations and their influence on network neutrality.

**End-to-End Algorithms**

The Internet is commonly understood as an *end-to-end network*. Jerome Saltzer, David Reed, and David Clark formalized the term "end-to-end" in the article "End-to-End Arguments in System Design" in 1984 (Gillespie, 2006). They outlined a formal design principle for computer engineers to follow when developing data communications networks. Where most refer to the end-to-end as a principle, the concept clearly fits as a type of network relation. The relation prioritizes the ends of the network in order to ensure proper communication of messages. The end-to-end network relation holds that correct message delivery "can completely and correctly be implemented only with the knowledge and the help of the application standing at the end points of the communication system" (Saltzer, Reed & Clark, 1984: 287). Only the sender and the receiver can guarantee the accuracy of a message, since they alone know its contents. The popularization of E2E network relations celebrated the "stupid network" where the network did little else than ferry bits between the ends (Isenberg, 1998)[6]. The relation requires the network only to do its *best effort* to route a packet to its destination, but not to guarantee its transmission. In sum, the relation tends to downplay the importance of the actual network, and instead focus on the ends of the network to do most of the work in sending and receiving packets.

A "best effort" amounts to networks avoiding any knowledge of the contents of the packets and focusing on routing the packet to its final destination. The packet is layered to keep the bits related to the content of the message separate from the routing information. The TCP/IP packet datagram contains four layers. The first three layers contain information about the transportation of a packet over network, and the last layer contains parts of the overall message. The most accessible bits of the packet contain routing information, where the least accessible bits

contain content. The layering of the packet in this way purposely eases the amount of data E2E algorithms need to process. Most network processors only read the upper layers of the packet; thereby they operate according to the E2E logic.

The inability to know the contents of the message causes E2E algorithms to struggle when transmitting time-sensitive packets. The logic of E2E prioritizes the transmission of chunks of non-time-sensitive computer data[7]. The transmission of voice, then, presents a challenge to E2E network relations. Networks do not become aware of the priority of the packet and route it normally. Slower transmission would then have a greater effect on a voice conversation, than the transmission of a large file using peer-to-peer (P2P) sharing (Karaganis, 2007: 257-259). Don Bowman of the major deep packet inspection firm, Sandvine, makes a point that the Internet without management is "not a neutral network" because "certain bandwidth hungry applications introduce delays into the network that prejudice time sensitive interactive applications like voice over IP and online gaming, which consume relatively little bandwidth" (CRTC, 2009a). By "bandwidth hungry applications", he clearly means P2P file sharing as it takes advantage of the E2E ignorance of session overload.

No algorithm better encapsulates the consequences of the network relations of E2E than the P2P BitTorrent algorithm. BitTorrent has a recursive relation to E2E. P2P hackers have embraced the politicizations of E2E by developing software–attempting to defy censorship and create a network of equal peers (see Oram, 2001; Wu, 2003). BitTorrent algorithms operate with a strict version of the E2E—each computer on the network is treated as an equal node. Peers become the source of data, similar to user-generated content. Each peer might only have a few bits of the file, but, by sharing their few bits they contribute to a distributed swarm of peers sharing a common file. The BitTorrent algorithm co-ordinates the exchange of bits of a file between a swarm of peers; a node might assemble parts of a file from hundreds of other nodes. Further, non-sharing nodes have their connection throttled, forcing ends to become productive members of the networks. The network relations of P2P privilege the ends. Each node co-exists as an equal amongst its other nodes (Benkler, 2006: 418-429; Bittorrent, 2009). The logic establishes hundreds of connections between peers, known as sessions. E2E algorithms encourage multiple sessions because every end is a productive part, so their networks bloom laterally between ends that upload and download bits without concern for hubs or centers. The 2008/2009 Internet Study by Ipoque, a leading developer of network processors, found P2P traffic accounts for an average of 56.32% of the traffic in Africa, Europe, and the Middle East[8]. The explosion of connections creates considerable strain on the centralized aggregation hubs run by ISPs due to the unchecked expansion of sessions congesting networks.

Network congestion is a consequence of E2E network relations. Its algorithms ignore the urgency of the message to preserve the equal treatment of all packets and to prioritize the ends of the network. BitTorrent exemplifies these processes of networking because ultimately these networks depend on "conspicuous recombinant reproduction" where peers freely share information to populate the network (Vaidhyanathan, 2004: 21). As Clay Shirky stated in 2001, just after the demise of Napster, "peer-to-peer is not merely erasing the distinction between client and server. It's erasing the divide between consumer and provider as well" (Shirky, 2001: 35). In effect, E2E networks operate very differently from traditional broadcast networking that favours top-down network distribution. This difference has intensified as ISPs begin to offer value-added services and suffer crippling network congestion so that they require greater management of the network. The resulting conflict has fostered the resurgence of a second type of network relations and algorithms: Quality of Service.[9]

**Quality of Service Algorithms**

The network relations of Quality of Service manage bandwidth to ensure certain channels of communication receive sufficient resources to guarantee their successful operation. Most often, management adheres to the contractual obligations in place between customers and their ISPs that allow discrimination and prioritization of traffic. "Bandwidth hungry applications" must be managed in order to preserve the functionality of "well-behaved" applications. Assigning the labels "bandwidth hungry" and "well-behaved" involves a politics of inclusion and exclusion. As Graham writes, "while [traffic management] will allow a guaranteed quality of service to 'premium' users and prioritized services, even at times of major Internet congestion, those packets deemed unprofitable will actually be deliberately 'dropped', leading to a dramatic deterioration in the electronic mobilities of marginalized users or non-prioritized services" (2005: 568). The logic of QoS, in sum, intervenes in the flow of communication to distribute scarce bandwidth by prioritizing value-added services or de-prioritizing nuisances.

Quality of Service network relations originated in the telecommunications industry (Mansell, 1993). The industry has always maintained a concern with ensuring its level of service; in part, a response to the contractual obligations of the consumer, but also due to its history of operating a public service (Crawford, 2007; Gillespie, 2006). In an era of telephone monopolies, quality of service became a mission statement (Sterling, 1992)**.** Telecommunications firms championed an "end-system" model where the network takes responsibility for data delivery to fulfill their mission (Sandvig, 2006: 241-243). This perspective differs from the responsibility of networks to only do their *best efforts* in the case of E2E. As telecommunication companies began to administer data networks for governments, particularly in the United States, the "end-system" model evolved into a "virtual circuit" or "intelligent" network models. This logic dominated the data network research when ARPANET first suggested the radical idea of an end-to-end network and best efforts. Bell Canada championed a virtual circuits model as the *best* way to ensure reliable communication online and to optimize networks for time-sensitive applications, such as voice (Gillespie, 2006: 431-435).

The conflict between QoS and E2E began recently when network processors began utilizing QoS algorithms. Early Internet routing lacked the capacity to *impose* QoS on its traffic. The Internet Protocol did contain provisions for QoS, but implementation was optional. *Figure 1* depicts the QoS provisions in the Internet Protocol. Most routers could read the QoS information included in the header, but few networks enforced these instructions (Huston, 1999). QoS lacked enforcement because early Internet routing did not have the resource to assign QoS for complex, high volume network.

The shortcomings of QoS in TCP/IP drove innovation in the development of more powerful network processors (Barney, 2005; Karaganis, 2007). Network processors have become so sophisticated they can run parallel operations on packets; they can route packets and manage packets at the same. QoS algorithms co-exist with end-to-end algorithms. A brochure for the Cisco CRS-1 router, for example, boasts it provides "total separation of traffic and network operations on a per-service or per-customer basis" that allows "carriers to isolate the control, data, and management planes" with the "confidence that they can meet customer service-level agreements" (Cisco Systems, 2009). New routers such as the Cisco CRS-1 fill an urgent need for ISPs.

The need for QoS algorithms has intensified; driving the telecommunications industry to invest heavily to deploy these QoS network processors Canadian ISPs treat themselves as a

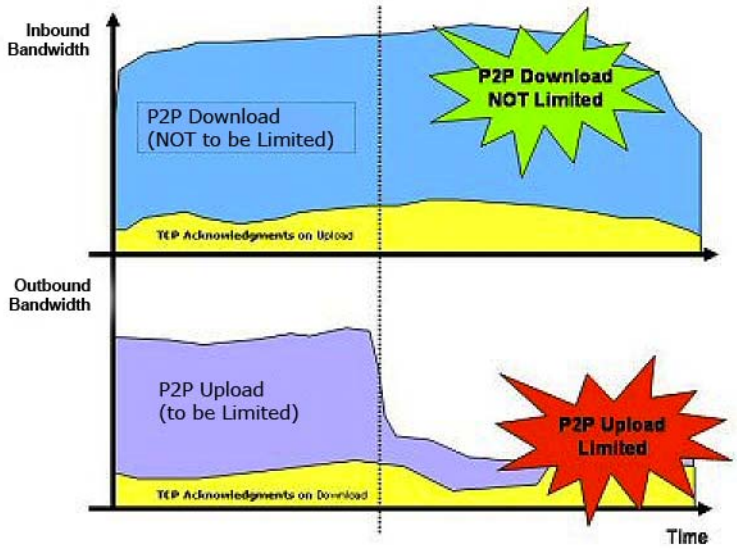
commercial service accountable with contractual quality of service expectations. Recently, these expectations have been hard to keep. ISPs cite the growth in file-sharing and bandwidth-intensive applications as technical developments that have degraded their quality of service (McTaggart, 2008, April 25-26). With only so much space in the pipe, the ISPs have invested in more sophisticated network processors that can impose QoS in tandem with routing packets. ISPs have to manage traffic "to ensure that P2P file sharing applications on the Internet do not impair the quality and value of [their] services" (Rogers Communications, 2009a). Their infrastructure investments, along with developments in the nature of network processors, have fueled the growth in QoS algorithms (Finnie, 2009; Ingham & Forrest, 2006).

***Figure 1:*** **Quality of Service Model**
Source: http://en.wikipedia.org/wiki/Quality_of_service.

| Priority Level | Traffic Type |
|---|---|
| 0 (lowest) | Best Effort |
| 1 | Background |
| 2 | Standard (Spare) |
| 3 | Excellent Load<br>(Business Critical) |
| 4 | Controlled Load<br>(Streaming Multimedia) |
| 5 | Voice and Video<br>(Interactive Media and Voice)<br>[Less than 100ms latency and jitter] |
| 6 | Layer 3 Network Control Reserved Traffic<br>[Less than 10ms latency and jitter] |
| 7 (highest) | Layer 2 Network Control Reserved Traffic<br>[Lowest latency and jitter] |

Two major new types of algorithms have facilitated the growth of QoS networking: deep packet inspection (DPI), and deep flow inspection (DFI) (Finnie, 2009). DPI algorithms, as its name implies, embed *deep* into the packet. It can inspect, monitor, and manage all the four layers of the packet, including the Application Layer where the content resides (Parsons, 2008). Pattern recognition and packet storage allows DPI appliances to understand the content and the protocol of the packet. Better recognition of the packet allows for improved distribution of resources. They can identify an illegal MP3 transmitted using a peer-to-peer file-sharing protocol or a prohibited word on a web page and allocate speeds accordingly. For instance, a German Internet Service Provider (ISP), named Wilhelm.tel, needed to curb the amount of file sharing on their networks[10]. They installed the Allot Communications NetEnforcer AC-1000 to limit the amount of bandwidth P2P uploading. *Figure 2* illustrates the amount of P2P uploading bandwidth reduced as a deep packet inspection algorithm recognized and shaped P2P uploading. The ISP testifies, "we instantly reduced traffic consumption by 150 Mbps and reduced costs by 10,000 Euros (US $12,000) per month" (Allot Communications, 2006).

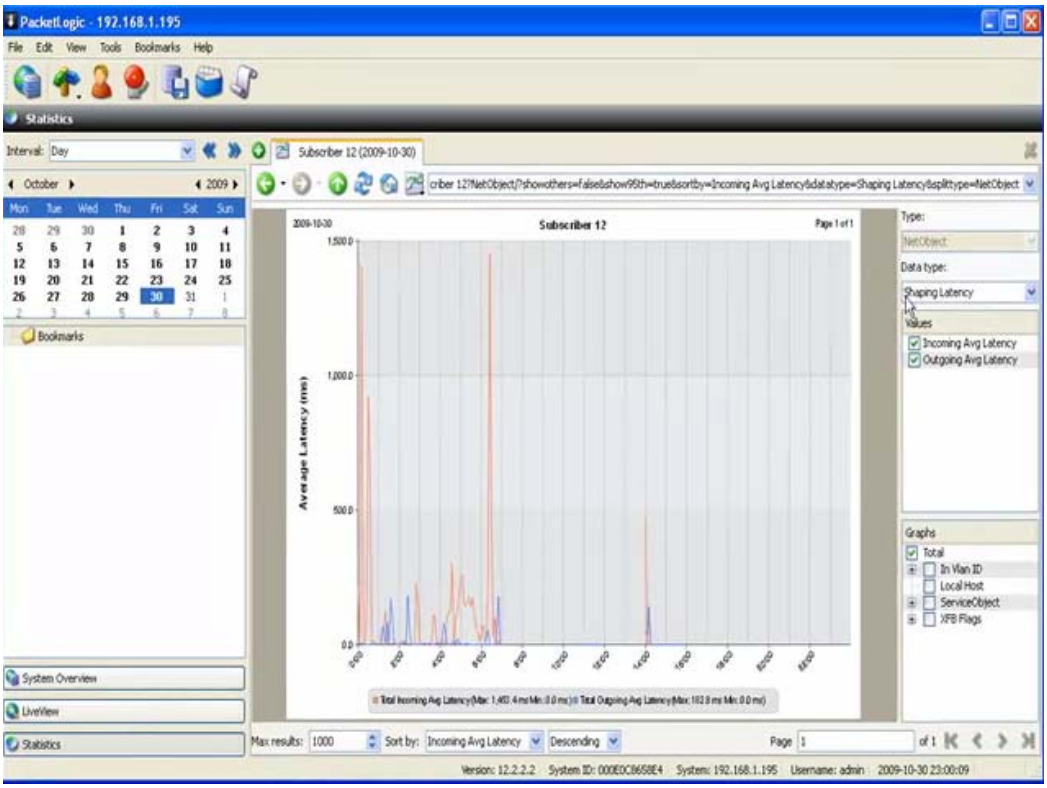
***Figure 2:*** **Wilhelm.tel's Bandwidth Savings**
Source: (Allot Communications, 2006).




However, DPI "is a black art in which both false positives and false negatives are unavoidable" (Finnie, 2009: 8); users often encrypt their packets to elude packet inspection. The industry responded with a heuristic to identify applications by the patterns in their packet flow. A Skype conversation sends packets at a different rate than browsing the web. *Figure 3* comes from a promotional video for Procera Network's Packet Logic Suite. The chart in the figure visualizes a flow of packets from a single user. Flow inspection allows networks to monitor the flow of a single user, not just the separate packets themselves to identify and manage certain channels of communication. These two components increase the capacity of networks to impose QoS by improving how algorithms identify the content of its inputs (Procera Networks, 2009).

The two types of detection algorithms enable policy management algorithms to create tiers within IP networks. Policy management is a "broad concept because it 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, customers, and applications" (Finnie, 2009: 12). Policy algorithms allow Internet Service Providers to tier their customer base, so some consumers have a *gold-tier service*, while others have a *platinum-tier*. Higher tiers might receive bandwidth priority. Further, some traffic, such as spam, worms, or P2P, might be seen as threats to the network and policies would slow or stop them. The list of rules dictates the response of routers to certain traffic patterns. A rule might rely on DPI to recognize a form of traffic, and utilize policy servers running QoS algorithms to slow its movement (Procera Networks, 2009).

***Figure 3:*** **Flow management in Procera Networks Packetlogic**
Source: (Procera Networks, 2009).




Creating tiers, in effect, illustrates QoS networking. All major Internet Service Providers in Canada, except for Telus, use deep packet inspection. For example, Bell Canada throttles BitTorrent traffic during peak hours. Bell's networking code identifies BitTorrent packets or even patterns in packets equated to BitTorrent communication (Bell Canada, 2009). Identified packets receive less bandwidth and, to the user, move slower on the network. Quality of Service algorithms not only slows P2P traffic, but also enables value-added services. Canadian ISPs have utilized the technology to prioritize their own services. Cogeco offers a prioritized voice-over-IP service, Rogers has new video-on-demand, and Bell also offers streaming TV. If P2P exemplifies the logics driving E2E, then video-on-demand exemplifies the applications in QoS. Centralized content producers and distributors feed content to the consumers existing at the ends of the network. This content travels as prioritized traffic on commercial networks (CRTC, 2009a).

The growth of QoS algorithms and their widespread deployment in Canada illustrates a second form of networking online. QoS favours the networks, the connections. The hubs and the center, not the ends, become the priorities of the network. Production in this network, for the most part, depends on industries, corporations, and established actors with access to the centers. E2E algorithms, in contrast, favour the ends; user-generated content, free software, and P2P all depend on empowered ends. The network neutrality controversy, then, can be described as a struggle over network relations of ends versus network relations of centers. The following section highlights the aspects of the controversy embedded in the algorithms of the Internet.

**Network Neutrality as the Struggle between Processes of Networking**

The network neutrality controversy takes on more depth when considering how these two processes compete to process packets and to shape networks. Privileging the ends favours home computers and peer-to-peer networking, whereas privileging the connections favours central servers and infrastructure. *Figure 4* depicts the resulting networks from their processes. Quality of Service generates a centralized network (A) with a strong central server. Its centripetal forces aggregate traffic into hubs that serve dependent nodes. The distributed network (C) illustrates the swarm mentality behind E2E networking. The network emerges from the centrifugal forces of algorithms, like BitTorrent, that push content away from any center. The centripetal and centrifugal forces both constitute the Internet. Its form, then, appears more like a decentralized network (B) with hubs, but also with de-centered swarms. Their co-existence creates the tensions, conflicts, and obliterations that have manifested in the network neutrality controversy.

***Figure 4:*** **Three types of networks**
Source: http://www.uvm.edu/~tstreete/Courses/Soc43/pages/lecture_radio.html.

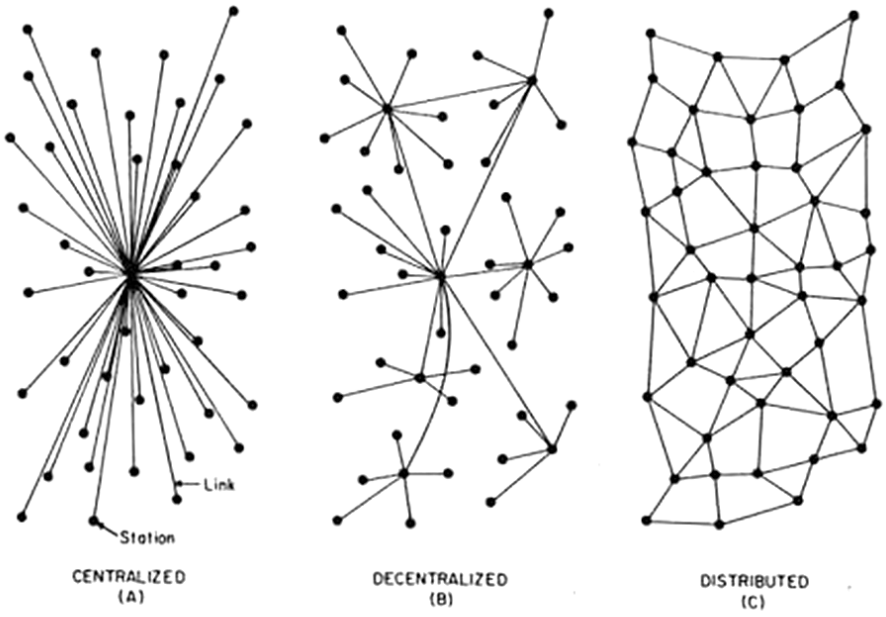
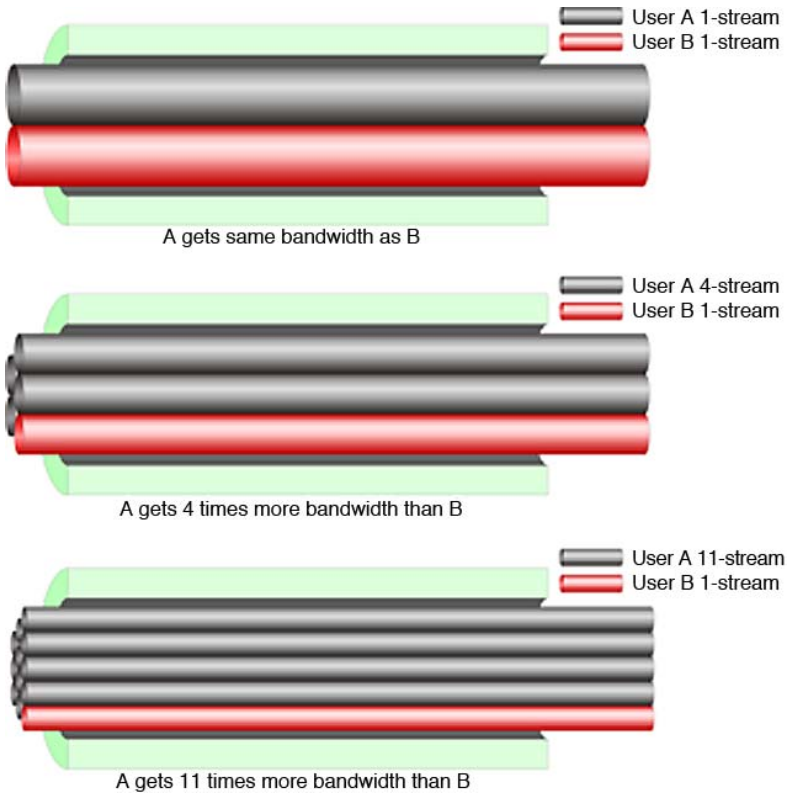



FIG. 1 — Centralized, Decentralized and Distributed Networks

Canadian ISPs' struggle with BitTorrent best exemplifies how the co-existence of the two processes of networking manifest in the controversy. In Bell Canada's recent filing to the CRTC, they describe P2P file sharing as a corrosive technology that uses a "disproportionate amount of bandwidth compared to other types of traffic" (Bell Canada, 2009). In the diagram below, Bell illustrates their argument through an interpretation of a broadband pipe. Given a limited amount of space in the pipe, Bell expects one computer to establish a limited number of connections to other hosts—from a node to a major server. The top of the pipe illustrates a fair network, in Bell's opinion, where a few connections exist. In contrast, BitTorrent creates a swarm of connections between many users. The bottom of *Figure 5* illustrates how BitTorrent traffic expands between peers—establishing hundreds of connections to share different bits of the same

file. The increase in connections between peers strains the capacity of bandwidth pipes. The figure illustrates the two processes of networking at work. The end-to-end network relations expand centrifugally where one node connects to many (one-to-many), whereas the Quality of Service relations contract centripetally where many flow to a single network center (many-to-one).

***Figure 5:*** **Bell's Internet Pipe**
Source: (Bell Canada, 2009).




The two network relations have different responses on how to handle strain on network resources. QoS networking requires a deliberate choice on the part of network owners to allocate resources, whereas E2E avoids making a decision. By moving the allocation of network resources under the dominion of network administrators, QoS networking conflicts with the ambiguous networking of E2E that leaves the decision of resource allocation to the ends. The technical ability of the network to decide on the ideal resource distribution translates into network owners making decisions about the nature of Internet communication. Rogers Communications argues peer-to-peer file sharing is "the least effective method of transmitting data. The cost of bandwidth on the last mile access network to the home is much greater than the cost of bandwidth in a traditional file server" (Rogers Communications, 2009b). Since their network clearly favors a hub, it should come as no surprise that both Rogers and Bell both have begun a video-on-demand service. While there is no explicit link between degrading P2P and promoting a new digital mall, their attitude certainly reveals a trajectory for network

development with network owners having more control over the priorities of the network. To be fair, their activities are not sinister, but do constitute a radically different network form.

One might argue that the E2E model attempts to create an infeasible network, and the QoS model is a more practical network; however, such a critique ignores the complexity of the network—the intertwining of desktop computers with backbone routers. Both models obfuscate aspects of the Internet's complexity. To begin, E2E networking, to be clear, does not correspond to the commercial construction of the Internet in Canada (or elsewhere probably) as seen in *Figure 6*.

***Figure 6:*** **The Bell Network**
Source: (Bell Canada, 2009).

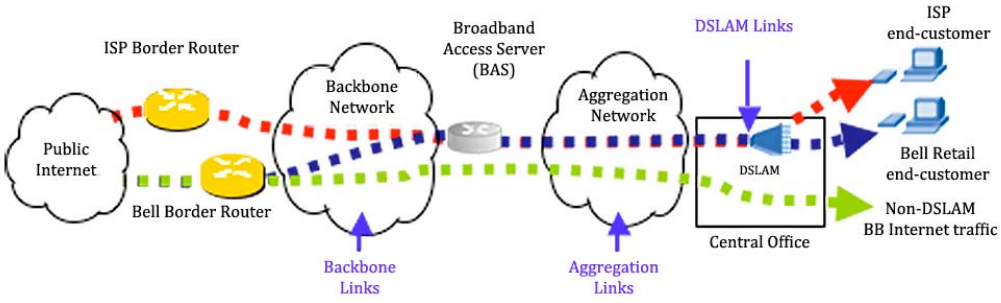



*Figure 6* depicts a Bell representation of their network. Home users connect to various tiers that eventually connect to the Internet backbone. The ends of the network are truly the ends of the networks; only capable of connecting to each other by traveling first to the central hub. Legitimately, P2P strains the resources of residential ISPs by overloading the hub to connect to each other, especially since ISPs oversell network capacity based on their traditional revenue models (McTaggart, 2006, September 30). At the same time, QoS omits the "generative capacity of the ends" (Zittrain, 2008). File sharing would not be such a problem if users did not have the capacity and the desire to share information. The ends play a vital part in the Internet and cannot be assumed to be irrelevant. In other words, the E2E model overlooks the connections, but fully recognizes the ends. The QoS model devalues the ends as contributors to the network in favour of centralized hubs serving content and ensuring proper transport. These tensions are political—a source of conflict, not consensus.

Since neither E2E nor QoS completely describes the Internet they should not be seen as answers, but they should be understood as part of the controversy. Controversies "enrich democracy" and "are powerful apparatuses for exploring and learning about possible worlds" (Callon, Lascoumes, & Barthe, 2009: 28). Recognizing the different politics of networking brings to the forefront algorithms as an actor in the network neutrality controversy. Neither algorithm is more at home or more part of the Internet than the other—one does not solve the other. Pundits on both sides would be wise to remember, "the question is no longer whether or not a solution is good; it is a question of how to integrate the different dimensions of the controversy in order to arrive at a 'robust' solution" (Callon, et al., 2009: 32). Such a solution should keep in mind the advantages and disadvantages of both algorithms and network relations.

## Conclusion

The network neutrality controversy can now be seen less as a cleavage between open and closed networks than as a point of collision between different processes of networking. Perhaps the answer to network neutrality will not come from policy, but from the dominance of one algorithm over the other. If QoS applications, such as on-demand video and VoIP, become the default use of the Internet then E2E might simply fade away as inefficient. This is a very real possibility as ISPs generate new streams of revenue through rich content delivery. Yet, E2E has influenced a dynamic participatory culture online as well. Piracy and user-generated content have changed popular culture. If participatory culture continues to thrive, the appeal of QoS video-on-demand applications might evaporate. To continue to think of network neutrality without a sense of the algorithms working online ignores a central site of conflict and a point of entry for a broader study of the controversy.

Finding a robust solution entails incorporating the cultures involved with each algorithm. QoS and E2E have imbricated with vastly different cultures. QoS circulates amidst telecommunications firms, digital content providers, and the networking technology industries. Its proprietary algorithms are developed by private industries associated with the commercial provision of the Internet (Barney, 2004). Conversely, E2E emerged from the altruism of engineers and Netheads, and continues to thrive as its politicization inspires new generations to create even more political software (Kelty, 2008). In contrast to the economics of QoS, the most successful E2E algorithms, namely P2P, began as political statements. These different sides of the controversy enter through a focus on algorithms. Who produces them and for what reason? What are the ramifications of privileging one algorithm over another? This paper has offered a window into a large and complex world of the software side of networking.

The outcome of the network neutrality controversy will ultimately influence communication online. Models of networks manage human communication; algorithms produce and reproduce forms of media power (Graham, 2005; Mulgan, 1991; Winseck, 2002). Stabilizing a position on network neutrality will restructure the Internet. Speculation on the Internet's future—the future of communication online—fuels the controversy. Scholars imagine the Internet fostering a renewed democratic culture (Balkin, 2004; Benkler, 2006; Lessig, 2004), while companies worry it will no longer be profitable to operate online (Mason, 2008). Attending to the controversy allows these issues to come to the forefront, and studying algorithms attends to a crucial side of the debate.

For the network neutrality controversy to have relevance it must, to borrow from Sandvig (2006), adopt a "normative concept" of what algorithms are supposed to do. Network neutrality advocates have the most to lose if this is the case. The term *network neutrality* obfuscates the politics of its algorithms. In actuality, a network neutrality principle makes a political stand by preserving the generative, perhaps radical democratic, aspects of the Internet. Participatory culture, social media, citizen journalism, and the creative commons depend on users being able to upload, broadcast, and share freely. Peers are the productive ends of the network. Since network neutrality would require increases in bandwidth to facilitate its generative capacities, the pro-Network Neutrality movement needs to embrace the network as a political project or else it stands to lose to the economic rationalities that dictate the network today.

**Notes**

* The author wishes to thank Greg Elmer, Ganaele Langlois, Zachary Devereaux, Catherine Middleton, Christopher Parsons, and Isabel Pedersen for their support in bringing the paper to fruition.

1 The circumstances of Bell's action fueled anti-competitive concerns. The public broadcaster in Canada, the CBC, had just begun to offer its television shows via peer-to-peer file sharing. Bell's traffic management throttled the CBC's peer-to-peer distribution. The throttling has been seen as market interference. Bell Canada owns a share in the CBC's major competition, CTV Globemedia. Accusations of anti-competitiveness also included debate over broadcast models. Peer-to-peer distribution can be seen to compete with television broadcasting and on-demand services (see Mason, 2008).

2 See Longford (2007), McTaggart (2008, April 25-26), and the Special Section on Net Neutrality in the 2007 issue of the International Communications Journal (http://ijoc.org/ojs/index.php/ijoc/issue/view/1/showToc).

3 Stabilization refers to a term developed by Bruno Latour. He uses the term in the context of the development of the Aramis transit project as a way to explain how enrolling more actors in the project increased its stability. The more documents, studies, and technologies enrolled in the project, the more stable it becomes (Latour, 1996: 46-50). The same applies to cultures that enroll policies, technologies, and studies to stabilize their vision of the network.

4 Mansell (1993) informs the discussion between code and its interpretation. She argues that strategic models (imperfect competition) and idealist models (perfect competition) of how the market will develop have driven the telecommunications industry. Code, by comparison, suffers from idealist and realist interpretations; the former holds that code lacks a politics, where the latter regards code as a technical construction imbued with political goals.

5 Different implementations of packet switching varied in their network algorithms. ARPANET, the network developed by the Advanced Research Projects Agency (ARPA), initially preferred active network management—a virtual circuit—where the network managed communication enough to ensure its safe delivery. Their approach differed from other networks, particularly one started by the French government in 1972. The Cyclades network, named after the group of islands in the Aegean Sea, aimed to connect "isolated 'islands' of computing" (Abbate, 1999: 124). The network favoured less involvement by the network. It did not ensure the delivery of packets, rather, the simple algorithms did their best effort to route packets safely and left message control to the ends of the network. Eventually, the result of best-efforts algorithms became the de-facto standard with the articulation of the end-to-end principle and the stabilization of Internet Protocol Suite (TCP/IP).

6 The celebration of the stupid network came just as telecommunication firms had invested heavily into the notion of an intelligent network (See Mansell, 1993).

7 Interestingly, Salter, Reed, & Clark do not consider the E2E principle incompatible with voice communication; rather, "an unusually strong version of the end-to-end argument

applies". They reason, "if low levels of the communication system try to accomplish bit-perfect communication, they will probably introduce uncontrolled delays in packet delivery". In other words, networks should do less to ensure the proper delivery of packets and let the ends of networks sort out lapses in communication. Etiquette, not intelligent networks, solves disruptions as they suggest that "the high-level error correction procedure in which one participant says 'excuse me, someone dropped a glass. Would you please say that again?' will handle such dropouts" (1984: 284-285).

8 For a full copy of the report, see: http://www.ipoque.com/resources/internet-studies.

9 This bias goes back to the origins of packet switching in computer data processing. Donald Davies at the National Physics Laboratory in England, one of the pioneers of packet switching, developed the communication method as an optimal model for the commercial provision of computer time-sharing services (Abbate, 1999). This bias might explain why mail emerged on the Internet before voice; it behaves more like a mail system as Bell illustrates above.

10 The Wilhelm.tel is a fairly simple case, but it provides the best illustration of the new network infrastructure. For more interesting examples, see http://www.allot.com/index.php?option=com_docman&task=cat_view&gid=88888896&Itemid=88888898.

---

**References**

Abbate, Janet. (1999). *Inventing the Internet*. Cambridge, MA: MIT Press.

Allot Communications. (2006). P2P control helps wilhelm.tel reduce broadband congestion and costs. Retrieved May 28, 2010, from http://www.allot.com/index.php?option=com_docman&task=doc_view&gid=41.

Balkin, Jack M. (2004). Digital speech and democratic culture: A theory of freedom of expression for the information society. *New York University Law Review, 79*(1), 1-58.

Barney, Darin (2005). *Communication technology*. Vancouver: UBC Press.

Barney, Darin. (2000). *Prometheus wired: The hope for democracy in the age of network technology*. Chicago, IL: University of Chicago Press.

Barney, Darin. (2004). *The network society*. Oxford: Polity.

Barratt, Neil, & Shade, Leslie R. (2007). Net neutrality: Telecom policy and the public interest. *Canadian Journal of Communication, 32*(2), 295-305.

Beer, David. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society, 11*(6), 985-1002.

Bell Canada. (2009). *Comment on public notice 2008-19: Review of the Internet traffic management practices of Internet service providers*. Retrieved March 15, 2010, from http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029804.zip.

Beniger, James R. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge, MA: Harvard University Press.

Benkler, Yochai. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale University Press.

Bittorrent. (2009). The BitTorrent protocol specification. Retrieved March 15, 2010, from http://bittorrent.org/beps/bep_0003.html.

Burgess, Jean, & Green, Joshua. (2009). *YouTube: Online video and participatory culture*. Cambridge: Polity.

Callon, Michel, Lascoumes, Pierre, & Barthe, Yannick. (2009). *Acting in an uncertain world: An essay on technical democracy*. Cambridge: MIT Press.

Canadian Radio-television and Telecommunications Commission (2008). *Telecom decision CRTC 2008-108: The Canadian Association of Internet Providers' application regarding Bell Canada's traffic shaping of its wholesale Gateway Access Service*. Retrieved March 12, 2010, from http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm.

Canadian Radio-television and Telecommunications Commission (2009a). *Hearings for review of the Internet traffic management practices of Internet service providers*. Retrieved March 15, 2010, from http://www.crtc.gc.ca/eng/transcripts/2009/tt0706.htm.

Canadian Radio-television and Telecommunications Commission (2009b). *Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers*. Retrieved March 12, 2010, from http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm.

Chun, Wendy. (2005). On software, or the persistence of visual knowledge. *Grey Room, Winter* (18), 26-51.

Cisco Systems. (2009). Cisco Carrier Routing System. Retrieved May 28, 2010, from http://www.cisco.com/en/US/prod/collateral/routers/ps5763/prod_brochure0900aecd800f8118.pdf.

Crawford, Susan P. (2007). Internet think. *Journal on Telecommunications and High Technology Law, 5*(2), 467-468.

DeNardis, Laura. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge: MIT Press.

Elmer, Greg. (2002). The case of web browser cookies: Enabling/disabling convenience and relevance on the web. In Greg Elmer (Ed.), *Critical perspectives on the Internet* (pp. 49-62). Lanham, MD: Rowman & Littlefield.

Elmer, Greg. (2008). Exclusionary rules? The politics of protocols. In Andrew Chadwick and Philip N. Howard (Eds.), *Routledge handbook of Internet politics* (pp. 376-383). New York: Routledge.

Finnie, Graham. (2009). ISP traffic management technologies: The state of the art (on behalf of Canadian Radio Television and Telecommunications Commission). Retrieved July 31, 2010, from http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm.

Frieden, Robert M. (2002). Revenge of the bellheads: How the netheads lost control of the Internet. *Telecommunications Policy, 26*(7-8), 425-444.

*Frontier*. New York: Bantam Books.

Fuller, Matthew. (2003). *Behind the blip: Essays on the culture of software*. Brooklyn, NY: Autonomedia.

Fuller, Matthew. (2008a). Introduction. In Matthew Fuller (Ed.), *Software studies: A lexicon* (pp. 1-14). Cambridge, MA: MIT Press.

Fuller, Matthew. (Ed.). (2008b). *Software studies: A lexicon*. Cambridge, MA: MIT Press.

Galloway, Alexander R. (2004). *Protocol: How control exists after decentralization*. Cambridge, MA: MIT Press.

Galloway, Alexander R. (2006). *Gaming: Essays on algorithmic culture*. Minneapolis, MN: University of Minnesota Press.

Galloway, Alexander R. & Thacker, Eugene. (2004). Protocol, control, and networks. *Grey Room, 17,* 6-29.

Gillespie, Tarleton. (2006). Engineering a principle: 'End-to-end' in the design of the Internet. *Social Studies of Science, 36*(3), 427-457.

Gitelman, Lisa. (2006). *Always already new: Media, history, and the data of culture.* Cambridge, MA: MIT Press.

Goffey, Andrew. (2008). Algorithm. In Matthew Fuller (Ed.), *Software studies: A lexicon* (pp. 15-20). Cambridge, MA: MIT Press.

Graham, Stephen D. N. (2005). Software-sorted geographies. *Progress in Human Geography, 29*(5), 562-580.

Halavais, Alex. (2009). *Search engine society*. Cambridge: Polity.

Huston, Geoff. (1999). *ISP survival guide: Strategies for running a competitive ISP*. New York: Wiley.

Ingham, Kenneth & Forrest, Stephanie. (2006). Network firewalls. In Vijay R. Vemuri (Ed.), *Enhancing computer security with smart technology* (pp. 9-35). Boca Raton: Auerbach Publications.

Introna, Lucas & Nissenbaum, Helen. (2000). The public good vision of the Internet and the politics of search engines. In Richard Rogers (Ed.), *Preferred placement: Knowledge politics on the web* (pp. 25-48). Maastricht: Jan van Eyck Akadamie.

Isenberg, David S. (1998). The dawn of the "stupid network". *netWorker, 2*(1), 24-31.

Kapica, Jack. (2008). Bell opens a large can of worms. *Globe and Mail*. Retrieved July 31, 2010, from http://v1.theglobeandmail.com/servlet/story/RTGAM.20080521.WBcyberia20080521192217/WBStory/WBcyberia.

Karaganis, Joe. (2007). The ecology of control: Filters, digital rights management, and trusted computing. In Joe Karaganis (Ed.), *Structures of participation in digital culture* (pp. 256-281). New York: Social Science Research Council.

Kelty, Christopher M. (2008). *Two bits: The cultural significance of free software* Durham, NC: Duke University Press.

Langlois, Ganaele, McKelvey, Fenwick, Elmer, Greg & Werbin, Kenneth. (2009). Mapping commercial web 2.0 worlds: Towards a new critical ontogenesis. *Fibreculture, 14*.

Lash, Scott. (2007). Power after hegemony: Cultural studies in mutation? *Theory Culture Society*, *24*(3), 55-78.

Latham, Robert & Sassen, Saskia (Eds.). (2005b). *Digital formations: IT and new architectures in the global realm*. Princeton, N.J.: Princeton University Press.

Latham, Robert & Sassen, Saskia. (2005a). Digital formations: Constructing an object of study. In Robert Latham and Saskia Sassen (Eds.), *Digital formations: IT and new architectures in the global realm* (pp. 1-33). Princeton, N.J.: Princeton University Press.

Latham, Robert. (2005). Networks, information, and the rise of the global Internet. In Robert Latham and Saskia Sassen (Eds.), *Digital formations: IT and new architectures in the global realm* (pp. 146-177). Princeton, N.J.: Princeton University Press.

Latour, Bruno. (1996). *Aramis, or, the love of technology*. Cambridge: Harvard University Press.

Lekkas, Panos C. (2003). *Network processors: Architectures, protocols, and platforms*. New York: McGraw-Hill.

Lessig, Lawrence. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. New York: Penguin Press.

Lessig, Lawrence. (2006). *Code: Version 2.0*. New York: Basic Books.

Longford, G. (2007, May). *'Network neutrality' vs. 'network diversity': A survey of the debate, policy landscape and implications for broadband as an essential service for Ontarians*. Paper for the Ministry of Government Services, Ontario.

Mackenzie, Adrian. (2006). Java: The practical virtuality of Internet programming. *New Media & Society, 8*(3), 441-465.

Manovich, Lev. (2002). *The language of new media*. Cambridge, MA: MIT Press.

Mansell, Robin. (1993). *The new telecommunications: A political economy of network evolution*. Thousand Oaks: Sage Publications.

Mason, Matthew. (2008). *The pirate's dilemma: How youth culture is reinventing capitalism*. New York: Free Press.

McTaggart, Craig. (2006, September 30). *Was the Internet ever neutral?* Paper presented at the 34th Research Conference on Communication, Information and Internet Policy George Mason University School of Law, Arlington, Virginia, U.S.A.

McTaggart, Craig. (2008, April 25-26). *Net Neutrality and Canada's Telecommunications Act.* Paper presented at the 14th Biennial National Conference on New Developments in Communication Law and Policy, Law Society of Upper Canada, Ottawa.

Moll, Marita & Shade, Leslie R. (2008). Telecommunication picks up speed on the free(market) way. In Teresa Healy (Ed.), *The Harper record* (pp. 405-407). Ottawa: Canadian Centre for Policy Alternatives.

Mulgan, Geoff J. (1991). *Communication and control: Networks and the new economies of communication*. New York: Guilford Press.

Oram, Andy. (Ed.). (2001). *Peer-to-peer: Harnessing the benefits of a disruptive technology*. Sebastopol: O'Reilly.

Parsons, Christopher. (2008). Deep packet inspection in perspective: Tracing its lineage and surveillance potentials. Retrieved July, 31, 2010, from https://qspace.library.queensu.ca/bitstream/1974/1939/1/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf.

Procera Networks. (2009). Products overview. Retrieved March 15, 2010, from http://www.proceranetworks.com/products-overview.html.

Ripeanu, Matei, Mowbray, Miranda, Andrade, Nazerano & Lima, Aliandro. (2006). Gifting technologies: A BitTorrent case study. *First Monday, 11*(11).

Rogers Communications. (2009a). *Comment on Public Notice 2008-19: Review of the Internet traffic management practices of Internet service providers*. Retrieved March 15, 2010, from http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029665.zip.

Rogers Communications. (2009b). *Response to Request to Interrogatory for 2008-19: Review of the Internet traffic management practices of Internet service providers*. Retrieved March 15, 2010, from http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1005723.zip.

Saltzer, Jerome H., Reed, David P. & Clark, David D. (1984). End-to-end arguments in system design. *ACM Transactions on Computer Systems, 2*(4), 277-288.

Sandvig, Christian. (2006). Shaping infrastructure and innovation on the Internet: The end-to-end network that isn't. In David Guston and Daniel Sarewitz (Eds.), *Shaping science and technology policy: The next generation of research* (pp. 234-255). Madison, WI: University of Wisconsin Press.

Sandvig, Christian. (2007). Network neutrality is the new common carriage. *Info: The Journal of Policy, Regulation, and Strategy, 9*(2/3), 136-147.

Sassen, Saskia. (2000). Digital networks and the state: Some governance questions. *Theory, Culture & Society, 17*(4), 19-33.

Shirky, Clay. (2001). Listening to Napster. In Andy Oram (Ed.), *Peer-to-peer: Harnessing the benefits of a disruptive technology* (pp. 21-37). Sebastopol: O'Reilly.

Sterling, Bruce. (1982). *The hacker crackdown: Law and disorder on the electronic frontier*. New York: Bantam Books.

Vaidhyanathan, Siva. (2004). *The anarchist in the library: How the clash between freedom and control is hacking the real world and crashing the system*. New York: Basic Books.

van Dijck, Jose. (2009). Users like you? Theorizing agency in user-generated content. *Media, Culture, & Society, 31*(1), 41-58.

Winseck, Dwayne. (2002). Netscapes of power: Convergence, consolidation and power in the Canadian mediascape. *Media, Culture, & Society, 24*(6), 795-819.

Wu, Timothy & Yoo, Christopher S. (2007). Keeping the Internet neutral?: Tim Wu and Christopher Yoo debate. *Federal Communications Law Journal*, *59*(3), 575-592.

Wu, Timothy. (2003). When code isn't law. *Virginia Law Review*, *89*(4), 104-170.

Yoo, Christopher S. (2004). Would mandating broadband network neutrality help or hurt competition? A comment on the end-to-end debate. *Journal on Telecommunications and High Technology Law*, *3*(1).

Zittrain, Jonathan. (2008). *The future of the Internet and how to stop it*. New Haven, CT: Yale University Press.

---

**About the Author**

Fenwick McKelvey is a PhD Candidate in the Communication & Culture program researching digital political communication, digital research methods, and Internet politics. His dissertation charts the politics of traffic management software—how it controls information and how it meets resistance. A graduate of the MA program in Communication & Culture, his MA work explored the code and politics of web2.0 by studying The Pirate Bay and Drupal. He holds a Joseph-Armand Bombardier Canada Graduate Scholarship.

---

***Citing this paper:***

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