INTERNET ROUTING ALGORITHMS, TRANSMISSION AND TIME: TOWARD A CONCEPT OF TRANSMISSIVE CONTROL

by Fenwick Robert McKelvey
Master of Arts, Toronto, 2008
Bachelor of Arts, Halifax, 2006

A dissertation
presented to Ryerson University and York University
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in the Program of
Communication and Culture

Toronto, Ontario, Canada, 2013

Author's Declaration For Electronic Submission Of A Dissertation

I hereby declare that I am the sole author of this dissertation. This is a true copy of the dissertation, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this dissertation to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this dissertation by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my dissertation may be made electronically available to the public.

Abstract

Internet Routing Algorithms, Transmission and Time:

Toward a Concept of Transmissive Control

Doctor of Philosophy, 2013

Fenwick Robert McKelvey

Communication and Culture

Ryerson University and York University

This dissertation develops the concept of *transmissive control* to explore the consequences of changes in Internet routing for communication online. Where transmission often denotes an act of exchanging information between sender and receiver, transmissive control theorizes transmission as the production and assignment of common times or temporalities between components of a communication system. Transmissive control functions both operationally according to how computational algorithms route Internet data (known as packets) and systematically according to how patterns in these operations express temporalities of coordination and control. Transmissive control questions how algorithms transmit packets and how transmission expresses valuable temporalities within the Internet.

The concept of transmissive control developed as a response to advanced Internet routing algorithms that have greater awareness of packets and more capacity to intervene during transmission. The temporality of the Internet is changing due to these algorithms. Where transmissive control has been made possible by the Internet's core *asynchronous* design that allows for many different temporalities to be simultaneous (such as real-time networks or time-sharing networks), this diversity has taxed the resources of the Internet infrastructure as well as the business models of most Internet Service Providers (ISPs). To bring the temporal-

ity of the Internet back under control, ISPs and other network administrators have turned to transmissive control to better manage their resources. Their activities shift the Internet from an asynchronous temporality to a *poly-chronous* temporality where network administrators set and manage the times of the Internet.

Where this turn to traffic management has often been framed as a debate over the neutrality of the Internet, the dissertation re-orientates the debate around transmissive control. Tactics by the anti-copyright Pirate Bay and Internet transparency projects illustrate potential political and policy responses to transmissive control. The former seeks to elude its control where the latter seeks to expose its operation. These components as well as the operation of transmissive control will be developed through a series of metaphors from the film *Inception*, the demons of Pandemonium, the novel *Moby-Dick* and the film *Stalker*. Each metaphor cooperate to provide a comprehensive discussion of transmissive control.

Acknowledgements

This dissertation results from four years of work undertaken in Toronto. I have benefitted from the generosity and the support of many who make this city such a vibrant intellectual environment. I would like to acknowledge some of those who have influenced or directly contributed to this project. Acknowledgements are the most important part of any work to me. I hope these few words demonstrate in small measure how much those listed below have nurtured me in this journey.

The Infoscape Centre for the Study of Social Media has been my true academic home. It should be the third university listed on my degree. I wish to thank all present and past members of the Centre including: Paul Goodrick, Peter Ryan, Steven James May, Joanna Redden, Yukari Seko and Paul Vet. You have all been wonderful peers – making a place often fraught with HVAC issues much more hospitable. A special thanks goes to the big guy Zachary Devereaux, to Alessandra Renzi for leading me down this metaphoric path for better or worse, to Erika Biddle for teaching me a little more about grammar among other things and finally to Ganaele Langlois who has had a tremendous influence on my research.

The Joint Program in Communication and Culture combines faculty from Ryerson and York Universities. I have benefitted from the support and kindness of faculty from both departments. Special thanks goes to Charles Davis, Anne MacLennan, Catherine Middleton, Colin Mooers, Isabel Pedersen and David Skinner. Each have been a source of inspirational to me and a reminder of the remarkable community possible at a university. Though not in the Communication and Culture program, Andrew Clement, Gary Genosko and Leslie Regan Shade have been tremendously supportive and generous with their time.

Some of Ryerson's finest staff have been tremendously giving with me. Chapter Four depended on the patience and technical support of Ken Woo and Ken Connell. Thanks to Jo Ann Mackie for guiding me through the processes of the Communication and Culture pro-

gram. A special thanks to Many Ayromlou for hosting me many times in my favourite place on campus – his office – and to Patrick Williams for keeping me in shape mentally and physically.

I have also been tremendously fortunate to have the support of colleagues beyond Toronto. I wish to thank Steve Anderson, Solon Barocas, Taina Bucher, Louis Carbert, Daniel Downes, Joanna Everitt, Daniel Kreiss, Susan O'Donnell, Christopher Parsons, Jeremy Shtern, Tamara Small, Neal Thomas and Kenneth C. Werbin. Thanks for listening to my ideas, sharing your own and creating a dialogue that I hope to sustain over the years to come.

Friends and family have been vital to keeping me going over the years. Thanks to my family – Mom, Dad, John and Lauren – for putting up with their flaky son/brother long enough to see me actually finish school and to Jillian Witt for being a rainbow in contrast to some of the bleaker hues of writing. Luke Simcoe and A. Brady Curlew both deserve a special nod for keeping me in good spirits and honest.

The final words go to my committee who have taught me so much. Thanks goes first to Avner Levin and Darin Barney for serving as externals on my committee. You both offered insight that will drive my future work. Robert Latham and Barbara Crow both served as committee members and both represent thinkers to whom I aspire. I am very grateful for all your time, discussion and feedback. Though there is no formal dedication, no person is more important to this work or to my time in Toronto than Greg Elmer. Thank you for being my supervisor and my friend.

Table of Contents

List of Figures

List of Appendices

Chapter One: Introduction

An Introduction to Transmissive Control

Ringing bells announce the hour of the day. Serfs and nobles share in this instant of time as the hour sounds out. Their labours continue, but now with a common rhythm. Creating this common rhythm illustrates the function of communication systems. According to Raymond Williams, communication acts to "make common to many, impart" (1976, p. 72). Punctual ringing of bells impart an order by sounding out a common time. Monasteries ringing bells in medieval Europe, according to Lewis Mumford, "helped to give human enterprise the collective beat and rhythm of the machine; for the clock is not merely a means of keeping track of the hours, but of synchronizing the actions of men" (1934, p. 14). The transmission of a tone by a ringing bell imparted a collective rhythm to coordinate and control those in audible range. Without the sound of a bell, serfs and nobles would fall out of synchronization with this rhythm. Western civilization depended on its collective beats necessary to coordinate modern society. This dissertation questions the power of transmission to *control* social times though it focuses on broadband not bells.

Bells illustrate how communication systems have certain capacities of transmission that afford kinds of social control. A bell on its own merely resonates a sound, but rung punctually its chimes allowed people to arrive to work on time or get paid by the hour. Communication systems of all kinds manifest control by expressing these collective rhythms through systematic transmission. This control is a productive capacity of a communication system that enables communication within certain limits or conditions; rather than something to be avoided, it is integral to communication. Communication systems, like bell towers, have lim-

its to their capacities of transmission and control. Bells could only synchronize people in audible range. Even then, a bell tower could not control the audience within this range. How bells transmit a sound and control the affairs of a parish is a matter this dissertation addresses through its concept of *transmissive control*. It questions how forms of transmission function systematically to create and control social times. This dissertation specifically questions how the Internet involves an advanced form of transmissive control.

Advances in communication often involve the control of transmission. An early experiment in electrical communication began when King Louis XV of France summoned an audience of one hundred and eighty of his guards. Guards joined hands as instructed by the overseer of the experiment, Jean-Antoine Nollet, and, once commanded, one guard grabbed a wire connected to an early battery. His contact with the wire sent an electric charge through the guards – a shock that they were "all [s]ensible of it at the [s]ame In[s]tant of Time" (Needham, 1746, p. 256). Electricity coursed through the bodies of the guards and united them in a common moment of shock. A letter to Royal Society of London listed the experiment as one of many on "communicated electricity" performed in France in 1746 (Needham, 1746, p. 255). Later that year, Nollet conducted another trial where he arranged 200 monks in a circle 1.5 miles in circumference. Each monk held on to an iron wire, soon electrified. Again their bond transmitted an electrical pulse, shocking the monks at once. Electricity, as the experiment observed, could be communicated over large regions instantly. The observation grounded the science of electricity and led to the development of the electrical telegraph (Blom, 2010, p. 152; Elsenaar & Scha, 2002; Standage, 2007, pp. 1–2). National telegraph networks "permitted for the first time the effective separation of communication from transportation" according to James Carey (1989, p. 157). Electrical cables and other new media afford greater control of transmission, thereby its conditions to control the times of coordination and cooperation.

The Internet involves an even more complex form of transmissive control than bells or telegraph wires. More than 250 years after the experiments of Nollet, a gamer logs into the massive multiplayer game *World of Warcraft* using the telegraph's successor, the Internet. The game requires a vast orchestration of computers and networks to simulate its virtual world. Gamers explore a giant virtual world full of dragons, orcs and elves with their personal avatars. Each click of their mouse interacts with other players or fights virtual monsters. Layers of computer mediation create a system of transmission so this virtual world binds gamers together just as an electrified wire did to Royal Guards. Computers encode and transmit their inputs to central servers that coordinate players in the game. Fibre optic lines and copper cables transmit all these various inputs between the millions of online gamers. Even though movements arrive as fragmented bits of information or packets, computers interpret and order packets so gamers experience a world at the same instant as their peers. Computers at each end encode and decode the motions of players to integrate individual actions into a simultaneous gaming world. Without this sophisticated orchestration, players would inhabit separate worlds out of synchronization with each other. Their virtual world is a complex expression of distributed computation and coordination based on decades of scientific thought (see Galison, 2003).

Disruptions or miscommunications demonstrate the complexity of Internet transmission. Lag, for example, is a bane to gamers trying to coordinate their missions. Delay in synchronizing player and server causes avatars to stutter and become out of synch with their team. Usually lag occurs due to the delay caused by distance or even the qualities of an ADSL or cable connection – problems usually associated with the transmissive properties of physical media. Perhaps gamers of *World of Warcraft* using Rogers Internet assumed the same when troubleshooting the source of their lag. Lag had proven to be a major problem for Rogers

Internet customers, enough that Teresa Murphy of the Canadian Gamers Organization investigated the issue. They discovered Rogers Internet traffic management software caused the lag (Roseman, 2012). Algorithms – a term for the autonomous functions of software – in Roger's network identified *World of Warcraft* traffic as peer-to-peer traffic and, as a result, *throttled* its transmission rate. Many ISPs perceive peer-to-peer as a threat to their emerging on-demand services. Speaking at the 2010 Canadian Telecom Summit, David Purdy, then Vice-President of TV/Video Product Management for Rogers Communications admitted, "there is some benefit in managing our networks just in terms of cutting down [peer-to-peer] traffic" (Purdy, 2010, np.). His words reveal how transmission can involve deliberate orchestrations of communication to foster or suppress certain rhythms. Throttling algorithms did not target all applications on the network, only peer-to-peer applications.

Algorithms in communication systems separate transmission from its medium, just as electricity separated transmission from transportation. Where once wires ensured a message was routed from sender to receiver, now algorithms deliberately control the transmission of the message to shorten or lengthen its passage through networks. Algorithms allow desperate gamers to simultaneously interact in a virtual world similar to how a shock conducted over a wire created a simultaneous experience of pain between monks and guards. The difference between the telegraph and the Internet illustrates how communication systems have advanced this control of transmission from the broadcasts of the bell to the narrowing of hands on a common wire to the sophisticated control by algorithms.

Algorithms enact very advanced forms of transmissive control. Internet transmissive control *produces and assigns temporalities to transmissions utilizing algorithms for data profiling and networking*. New traffic management algorithms enact a more dynamic or *modulating* control capable of redlining certain traffic like peer-to-peer while promoting on-demand services. They

can decide how much bandwidth to allocate to specific forms of communications. More bandwidth takes less time and less bandwidth takes more time. Managing bandwidth allows Internet transmissive control to create different rates of transmission at the same time. The Internet does not have just one form of transmission, but algorithms allow for many different times to coexist through different conditions of transmission. They allow for *asynchronous communication* on the Internet with many temporalities since its limits of transmission no longer reside in the physical properties of a wire.

Asynchronicity has been a source of tension and conflict. Internet Service Providers have begun to optimize their networks through transmissive control to tier and manage the many times of the Internet. Critics worry this use of transmissive control will create inequities of access where some users pay for high speeds, where others muddle their way through the Internet. They have called for a *Network Neutrality* rule that would require networks to transmit all Internet traffic with equality. Despite years of lobbying, the rules remain no closer to being implemented and the uses of transmissive control change as Internet Service Providers tweak and hone their shaping techniques. A focus on the transmissive control, then, offers a different approach to the matters of Network Neutrality. It seeks to conceptualize how the nature of Internet transmission operates and how it produces valuable temporalities.

To understand the stakes of asynchronicity requires a more precise sense of the temporal aspects of transmission. Synchronization – as in imparting a common time – is just one way to describe the collective effects of transmission. How might other more complex expressions of time be considered? James Carey argued that the telegraph and later the telephone participated in the re-orientation of stock markets from arbitrage to futures beyond just synchronizing the nations' clocks. The rate of electric currents outpaced the movement of physical goods that once allowed traveling vendors to buy low in one location and to sell high in another loc-

ation (1989, pp. 166–171). Electrical transmission synchronized prices across the United States. Communication systems not only allowed the greater synchronization of time, but also the concentration of temporal control in specific regions (cf. Castells, 1996, pp. 410–418). Access to these times had value. When New York worried that the telephone would allow brokerage firms to move to Boston, they introduced a thirty second delay to *excommunicate* firms in Boston from trading at the same time as firms in New York. Carey offers a sense of the economic function of communication media, one based on mediating access to a synchronized present. If the telegraph synchronized the present, how might transmission synchronize the past or future? More politically, how does it exclude forms of cooperation and coordination? To answer these questions, the dissertation introduces the term *temporal economy* to describe how transmission conjoins past, present and future to create valuable times of communication and excommunication.

Internet service providers and other owners have recognized the value of the Internet's transmissive control to create their own temporal economies. When ComCast, a major American Internet Service Provider, trademarked "We Own Faster" to market their high-speed Internet service, it raised important questions about the neutrality of the network in transmitting messages – a matter of transmissive control. Just prior to the "We Own Faster" campaign, the Electronic Frontier Foundation and the Associated Press had discovered ComCast had been deliberately slowing certain applications, specifically peer-to-peer (P2P) file-sharing. New traffic management algorithms had allowed ComCast to detect and throttle the transmission of certain kinds of Internet communications. ComCast did not announce these policies, nor did customers have an ability to opt-out. The revelation permitted another reading of the claims of the advertising campaign: ComCast did not just 'own faster,' but created 'faster' and, more to the point, created 'slower' using their newfound abilities to manage

Internet traffic. Faster and slower, as the advertisements assumed, had a value that customers would pay to access by presumably signing up with ComCast.

Transmissive control continually struggles to maintain temporal economies despite constant disruptions. All kinds of transmission have the potential to go out of control. Spam, viruses, errors, noise and theft all disrupt operations of transmissive control. Of all these threats, one of the most profound has been the work of *computer pirates.* Computer pirates and other hackers value *asynchronous* communications of the Internet and seek to protect it from being controlled by Internet Service Providers. Groups like The Pirate Bay in Sweden continually find new ways to sabotage transmissive control. These groups engage in a struggle over the very conditions of transmission to elude algorithms. Advanced traffic management struggles to overcome these challenges. Transmissive control involves both the systems it enacts and its own limits that it must continually overcome.

The stakes of transmissive control is more than sending and receiving, more than faster or slower. Communication creates a common time of being among its participants. The Internet hosts the collision of political visions, alters the circulation of cultures and sparks ruptures of production, such as free software and user-generated content. This diversity emerges and intersects through its expression in the common time, but the intensification of transmissive control will lead to tiering of the temporalities of the Internet. Internet Service Providers seek to create a temporal economy that removes collisions, contain ruptures and ranks diversities in this becoming; in doing so, they eliminate threats and insecurities even at the expense of creative and democratic expression (see Wolin, 2004, chap. 17). Keeping within the critical tradition of Communication Studies, this dissertation develops the concept of transmissive control to better explain the struggles on the Internet over its conditions of transmission.

Objectives

This dissertation studies the operation of transmissive control in wired Internet communications. Since most the backbone and mid-level infrastructure are fixed wired networks, the study of wired networks remains the best example of transmissive control. Future studies could apply transmissive control to discuss its particular implications to wireless transmission. This dissertation first situates transmissive control and the Internet by asking:

1. How does transmissive control contribute to the field of Communication Studies?
2. How does transmission express time? How does this expression take place on the Internet? What are the results?

This dissertation then develops a concept of transmissive control through the following questions:

3. What algorithms control the transmission of packets? How do they differ in this control? How do these algorithms function systematically?
4. What are the limits of this transmissive control? How do pirates elude[1] this control?
5. How do democratic publics confront transmissive control? How do the social sciences contribute to the representation of this control?

[1] The word 'elude' comes from the English translation of a conversation between Antonio Negri and Gilles Deleuze in the French journal Future Antérieur. The interview appears in English in the book Negotiations translated by Martin Joughin. He translates the original French passage "Il faut un détournement de la parole. Créer a toujours été autre chose que communiquer. L'important, ce sera peut-être de créer des vacuoles de non-communication, des interrupteurs, pour échapper au contrôle." as "We've got to hijack speech. Creating has always been something different from communicating. The key thing may be to create vacuoles of noncommunication, circuit breakers, so we can elude control". Joughin translates the French verb *échapper* as *elude*. It might also be translated as 'to escape', 'to dodge' or 'to run away'. For the original French interview, see http://multitudes.samizdat.net/Le-devenir-revolutionnaire-et-les. Thanks to Ganaele Langlois for help with this translation.

This dissertation aims to answer these questions through a literature review of studies of Internet control, a periodization of its emergence on the Internet and three cases related to its operation, elusion and representation.

This investigation of Internet transmissive control and its ensuing temporal economies relies on three interconnecting cases. Algorithms embedded in the Internet, as the first case shows, route packets – the standard unit of information – through networks. A packet's journey demonstrates how routing algorithms enact transmissive control and create a tiered temporal economy. This transmissive control, however, has its limits as shown in the second case of The Pirate Bay. The Swedish pro-piracy group eludes forms of transmissive control through peer-to-peer file sharing and, more recently, a virtual private network designed to cloak users' traffic from watchful algorithms. Yet, the nature of this struggle and of networks themselves remains outside the public view, so the final case questions the feasibility of public research into the state of the Internet. This case pushes the boundaries of social science research by questioning how the public could participate in research through different software tools. The research forms the basis of plans by the Canadian Internet Registry Association to establish an infrastructure for public broadband testing in Canada. Each case offers novel and innovative methods for the study of transmissive control.

This dissertation has six chapters building toward a more robust understanding of transmissive control. To help in this conceptual work, each chapter uses a central metaphor as a way to draw out and enliven the theoretical discussion. The metaphors change according to the facet of transmissive control under consideration. Metaphors have often helped describe communication systems. Media theorist Jussi Parikka (2007, 2010) uses metaphors of insects and viruses to discuss digital media and John Durham Peters (2010) suggests analog media have ghosts such as noise that haunt its information. These scholars hint at the many ways

metaphors aid in the study of communication systems. This dissertation uses the following metaphors:

- the nested dreams of the film *Inception* offer a means to visualize the asynchronicity of the Internet;
- the image of demon to represent the agency of algorithms in a communication system and to explore the conflicts between different kinds of algorithms;
- the novel *Moby-Dick* to explore the hunt for P2P networks and other forms of piracy;
- and the film *Stalker* to discuss and confront a system filled with oblique software processes.

These metaphors offer a way to characterize conceptual trends in the dissertation. As well, they have also been useful during the formulation of transmissive control.

This dissertation contributes to three major streams: communication theory, the emerging field of software studies (see Fuller, 2008) and the Network Neutrality controversy. The concept of transmissive control adds to theorization of the link between communication and control. Second, the investigation of software to control, to elude control and to publicize control contributes to software studies by researching networking software. Finally, the operation, the surrounding antagonism and the attempt for democratic representation of transmissive control interrogates the political economy of the Internet. In particular, bringing transmissive control to the public light engages with the forefront of the media reform movement and its attempts to engage the public in a call for more democratic communication sys-

tems[2]. This dissertation, in sum, adds theoretically, methodologically and politically to Communication Studies.

Literature Review

A number of disciplines have responded to the same advanced traffic management software motivating this study of transmissive control. Advances in traffic management software and hardware – specifically Deep Packet Inspection (DPI) – allow networks to recognize and manage IP flows with greater granularity and sophistication (see Parsons, 2011 for a literature review). Three fields in particular have touched upon these issues: the question of Network Neutrality in the field of Internet governance, the regulation of Internet censorship and surveillance as well as the field of communication studies. While each of these streams contributes to the knowledge of transmissive control, this section develops the question of control from within the Communication Studies literature.

Deep Packet Inspection and advanced traffic management software drive a debate in Internet governance over the optimal principles to regulate the Internet (Bendrath, 2009; Bendrath & Mueller, 2011; Benkler, 2006; Mueller & Asghari, 2011; Van Schewick, 2010; Wu & Yoo, 2007). The capacity of advanced traffic management software has provoked a debate over the virtue of a Network Neutrality principle that Wu first defined as "an Internet that does not favour one application (say, the world wide web), over others (say, email)" (2003a, p. 145). The term has become a central issue within research on Internet governance (Clark, 2007; Fulmer, 2006; Geist, 2008a; Hart, 2011; T. B. Lee, 2008; Marsden, 2010; Peha & Lehr, 2007).

Much of the literature on Network Neutrality frames the conflict as a question of open or closed networks. While this predominately legal approach contributes an important under-

[2] In Canada, see the work of the Open Media organization and its Save Our Net campaign at http://www.openmedia.ca/.

standing of the role of institutions, it understates the various forms and processes of control on networks – as if laws and policy only determine the functions of control online. The approach creates a binary divide between the open regulatory regimes without control and closed regulatory regimes with control. The divide obfuscates the functions of control within all network forms and suggests that network organizations might avoid control outright. This oversight is particularly evident in the following passage by Lessig when he states:

> At one extreme we might place the Internet – a network defined by a suite of protocols that are open and non-proprietary and that require no personal identification to be accessed and used. At the other extreme are the traditional closed, proprietary networks, which grant access only to those who with express authorization; control, therefore, is tight. In between are networks that mix elements of both. These mixed networks add a layer of control to the otherwise uncontrolled Internet. (2006, p. 34)

Lessig, problematically, positions control as the opposite of freedom. Opposing the two actually ignores their intertwinement. In a medium such as the Internet, digital control is necessary for computers to send information. The network is never neutral. Control is a productive form that enables communication within certain limits or conditions; rather than being something to be avoided, it allows the conditions integral to networks and must be studied. The weakness in the literature limits the applicability of the legal approach to capture the complexity of transmissive control.

Censorship and privacy researchers in International Relations have considered advanced traffic management software as threat to political freedoms. Authoritarian regimes deploy control technologies to censor the Internet, as well as security initiatives by liberal democracies (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, 2010). Privacy scholars have engaged with

advanced traffic management and Deep Packet Inspection as a problem of personal privacy. These devices collect and profile Internet usage for bandwidth management or even targeted advertisements (Bendrath & Mueller, 2011; McStay, 2010). The field has attracted many emerging scholars (Parsons, 2009; Paterson, 2009). Unlike Network Neutrality, the international relations approach has given in-depth consideration to the nuanced control of advanced traffic management software and its political economy, but much of this discussion returns to how national governments and other political actors adapt this software and its technical and discursive openness to its local context. They document, in other words, "how states are seeking to establish national borders on cyberspace" (Deibert & Rohozinski, 2010, p. 4). However, their emphasis on political freedoms, while vital research, tends to focus more on outright censorship than the nuances of transmissive control that deliberately avoids blocks. Cases drawn from the deployment of advanced traffic management software in liberal democracies differ from deployments in authoritarian regimes and thereby make contributions in their own right.

This dissertation fits within a third approach to advanced traffic management software from Communication Studies (Barratt & Shade, 2007; Sandvig, 2007). Traffic management software is a new form of control emerging among other economic, political or legal controls found in communication systems. Communication Studies concerns the "study of control and survival in social life" where control refers to the "internal organization of individual and group members" occurring through processes that "involve the social organization of relationships within a community" (Mosco, 1996, p. 26). Control involves both processes and augmenting larger systems occurring through these processes. Given the broad definition of control, it has been attributed to social, political, economic, legal and technological processes. These forms of control appear at work on the Internet, as laws (Lessig, 2006), acceptable usage

policies (Braman & Roberts, 2003), copyright (Gillespie, 2007), terms of service agreements (Sandvig, 2007) and systems of surveillance (Andrejevic, 2002), to name a few different techniques of control. Advanced traffic management offers a more precise usage of control – one embedded in the very operation of the communication system itself. This approach has a long history in Communication Studies and will be explored in depth in this dissertation.

Communication studies have always held an interest in the relation to communication systems as forms of social control (Barney, 2000; Braman, 2003b; Jowett, Jarvie, & Fuller, 1996; Mulgan, 1991). Hypodermic models, mass effects, culture industries – terms drawn from early work in Communication Studies – hinge on a sense of communication media to control society distinct from law, policy or politics. Research often proposed communication systems as a means to engineer utopias or as a catalyst for dystopias. The American pragmatists Walter Lippman and John Dewey exemplify one of the earliest perspectives of the potential of communication to control modern societies. In their writings, both worry that democracy had become incompatible with the public attention in mass society. A "mania for motor and speed" prevent publics from being attentive and capable democratic citizens (Dewey, 1927, p. 140). Communication systems could be a force to bring society back under democratic control. Walter Lippmann (1922) argues the media must control the "pictures people have in their heads" to guarantee a functional democracy. Communication perform an important function for social control by "manufacturing consent" (see Webster & Robins, 1989, pp. 341–344). John Dewey (1927), on the other hand, focuses on how media experiments could transform a mass society into a great community. Both Lippmann and Dewey only speculate on the actual infrastructure of a communication system, leaving media studies to later scholars.

Harold Innis (1950, 1951) famously argues that media influence the "dissemination of knowledge" over space and time. Media have a bias toward time or space – an analytic he lances

through an interpretation of Western history and the various civilizations that depended on certain technology to support "monopolies of knowledge" "Durable commodities", Innis states in reference to clay and stone, "emphasize time and continuity" and exhibit "a bias toward religion" (1951, pp. 33–34). His interpretation suggests that how media transmit knowledge manifest a social control. Biases depend on properties of the medium itself. Stone is heavy, but durable, so it endures longer, but travels slower. Papyrus is light and easy to transport, but the fibres of the plant rot over time – a space bias according to Innis. Although these media bias the development of civilizations, Innis worries that too much of a bias in space or time would cause the civilization to collapse. Media could become out of control and degrade the social control once sustained by their dissemination of information. Civilizations needed to find an equilibrium between time and space biases to ensure they would not collapse.

Marshall McLuhan (1994) embraces the work of Innis as a kind of *media studies*. Where Innis focuses ancient media, McLuhan favours modern technologies such as the television and the telegraph. He deviates from Innis by emphasizing how media *extend* human capacities of information processing and focusing more on the cultural effects of media. McLuhan recognizes the danger of technology becoming *out of control* by overextending the self to create new kinds of human anxieties and maladies, but he offered little advice other than Media Studies as a way to address the problems of media outside of control. Where McLuhan has an unquestionable legacy, Innis continues to resonate because of his emphasis on how communication's bias in its dissemination of knowledge has social and political consequences. Packets – like papyrus – afford certain patterns to the distribution of knowledge and allows for particular monopolies of knowledge. Space and time remains one of the most agile concepts to discuss how media and power, yet Innis is not the only scholar to chart this relationship. Just

when Innis and McLuhan realized the power of media, another scientific discipline came to the same realization.

Cybernetics and information theory forged an enduring bond between communication control and social control (Shannon & Weaver, 1949; Wiener, 1948). Norbert Wiener (1950) argues that computer-assisted communication allows for a system of management, responding to constant feedback and re-adjusting – a science he labels as *cybernetics*. "Its name signifies the art of pilot or steersman," Wiener wrote before adding, "that the word 'governor' in a machine is simply the latinized Greek word for a steersman" (1950, p. 9). Cybernetic control emphasizes the capacity to observe and intervene in an open communication system. Cybernetics frames communication as a system for control through observation and intervention. Wiener frequently uses the metaphor of a gunner tracking a moving target in large part because cybernetics sought predictive models of enemy fighter pilots to aid in the war efforts (see Galison, 1994). Control is not only a method of tracking, but also the capacity to pull the trigger at any given time. Wiener optimistically saw cybernetics as a way to avoid social decay or, in his terms, *entropy*. The constant and active control of cybernetics could create self-regulating systems that avoided entropy. Cybernetics spread across disciplines, including political science where Karl Deutsch (1966) links cybernetic with governance, proposing cybernetic systems of governance. Many nations attempted to implement cybernetics in government (Gerovitch, 2004). Chilean's doomed Allende government, for example, worked with cybernetic ist Stafford Beer (1974, 1975) to develop a communication system, known as Cybersyn, to manage a planned economy (Medina, 2011). Cybernetics, in short, ushered in the engineering of communication systems to the realm of politics.

Control did not acquire a critical dimension until well after the explosive growth of cybernetics, even though Wiener, for instance, worried about the use of cybernetics for military

purposes (Conway & Siegelman, 2005). James Beniger (1986) offers one of the first critical appraisals of what-he-called the Control Revolution. He argues that control arose out of a crisis in traditional techniques of management in the early 1900s, so industrial and social management required new technologies of control. Industrial crises, in short, required greater control over time. Where the basis of the information society underlying the Internet has often been cited as a recent development, Beniger argues "the basic societal transformation from Industrial to Information Society had been essentially completed by the later 1930s" (Beniger, 1986, p. 293). His book, in part a reaction to the hyperbole of the 'Information Revolution', situates advances in digital control as part of a longer Control Revolution. Periodization, however, is only one aspect of Beniger's larger theoretical contribution to the study of control.

Control, according to Beniger, "encompasses the entire range from absolute control to the weakest and most probabilistic form, that is, any purposeful influence on behaviour, however slight" (Beniger, 1986, p. 8). His definition of control distinguishes it from more political or coercive powers. It tends to be a softer and more probablistic form of power. Mechanisms of control contain *programming* to influence inputs towards specific goals. Beniger advocate control studies as a *teleonomic* epistemology in contrast to a *teleologic* one. Teleonomy derives from biologist Ernst Mayr who describea the teleonomic process as "one that owes its goal directedness to the operation of a program" and a program is "code or prearranged information that controls a process (or behaviour) leading it to a given end" (Quoted in Beniger, 1986, p. 41). Teleonomics describes society as the interactions between interconnected programs or logics that interact with specific goals in mind. He stresses the way these programs attempt to actualize a goal more than the actual goal itself. Studies of control, thus, focus on the invisible teleonomics of the programs that mediate the circulation of social actors.

His approach and theorization of control continues to resonate as a seminal study of the history of control technologies; however, his theories of control downplay its specific deployments of control and tends toward essentialism. Control appears as both a historical process and an elementary science, but the latter undermines the claims of the former. Peters (1988) questions his tendencies to treat information and control as fundamental rather than historical; his efforts attempt to position the study of control as a unified science. Beniger, or so Peters claims, follows the same dubious path as cybernetics by attempting to re-model the world around control. JoAnn Yates, on the other hand, argues that this broad scope "neglects specific interactions between communication or information technology and managerial needs" (Yates, 1989, p. xvi). She rectifies this perceived shortcomings in her own germinal work on communication and managerial communication.

Yates traces the history of formal means of communication in businesses from 1850 to 1920. She focused on a timeframe before the rise of computers when modern American firms had to adapt their management techniques for increased scales of operation. Historical organization communication – usually oral and informal communication – proved ineffective in managing the large firms emerging at this time. Hence her work focuses on the rise of formal communication techniques to bring firms back under control. Yates focuses on *managerial control* "over employees (both workers and other managers), processes, and flows of materials" that "is the mechanism through which the operations of an organization are coordinated to achieve desired results" (1989, p. xvi). Managerial control involved techniques of formal communication toward a *systematic management* of a business. The overall goal depersonalized the firm placing priority of the system over the individual. *Upward* communication referred to the mandated monthly reports where information moved from the lower to upper levels of the firm. *Downward* communication referred to written rules and orders that allowed superiors to

control the behaviour of their juniors. Finally, newsletters and in-house magazines sought to offset the de-personalizing communication flows by telling a human-side of the organization. These approaches emphasized how flow and direction of the transmission of information bind organizations together in particular configurations affording certain overall systems of control. Her approach re-asserts a relationship between routine mechanisms of control and the larger system they enact.

John Guillory (2004) adds to the program of research by Yates in a special issue of *Critical Inquiry* on *Arts of Transmission* (see Chandler, Davidson, & Johns, 2004). Guillory focuses on the memo as a particular style of communication distinct with the rhetorical tradition. The style of the memo ensured that different employees in an organization would write in a way to transmit information necessary for organization control. Guillory, as well as others, view transmission as a way of imparting knowledge across organizations or generations. This approach resonates with the long view of transmission developed by Régis Debray referring to cultural techniques of sharing knowledge across generations and times (see Debray, 2000; also Maras, 2008). These approaches are a more human than technical versions of control that functioning through literary styles. Although this line of research veers away from explicit discussion of control into questions of culture, it does indicate some of the other potential directions for the study control and transmission beyond the Internet itself. While Beniger, Yates and Guillory offer helpful theories of control, their attempts to ground control in the late-1800s and early 1900s should not imply that control stopped developing after their histories. Instead, critical approaches must address the advent of computing and cybernetics.

Darin Barney (2000) contributed one of the first major studies of control in networks. His version of control involves the capacity of networks to "enframe the world as a standing-reserve of bits because they demand that human practices be converted into bits in order

to be mediated and included in the institutional life of society" (Barney, 2000, pp. 230–231). Enframing technically occurs through encoding into binary sequences and packets. The approach provides a compelling critique to the hyperbola of networks as the saviour of political apathy. Where advocates dream of fibre pulling citizens into politics, enframing always precedes any activity on the web such that politics becomes a function of network technology converting any activity into a malleable reserve of bits. Problematically, the totalism of his Heideggerian approach understates some of the dynamics about the limits of control. The Internet appears as a one-sided system of total enframing. The approach, then, offers a strong problematization of the act of encoding and digitization, but overlooks the many resistances online such as computer pirates who create more complex articulations using the Internet than simply becoming a standing reserve of bits.

Within the late-20th century, Gilles Deleuze (1992, 1995a, 1998a) remains one of the most influential and provocative theories to critically approach digital control. A growing literature relies on Deleuze to study the evolution of control and its forms in digital communication (Bratich, 2006; Chun, 2006; Galloway, 2004, 2006; Guins, 2009; R. Jones, 2000). Deleuze developed the concept of *societies of control* as one answer to the problem of circulation that Foucault answered in his writings on discipline and biopolitics (see Foucault, 2007; Latham, 2012). Societies of control succeed disciplinary societies as a means to regulate circulation in open systems. Where discipline *fits* individuals into social molds to manage circulation, control *modulates* as a "self-deforming cast that will continuously change from one moment to another" (1992, p. 4). Modulation refers to a dynamic form adaptive to its variable inputs. Different social institutions cooperate to create a *continuous* system of control, in contrast to the specific deployments of control discussed by Beniger and the disciplinary enclosures of Foucault. As Deleuze writes, "the disciplinary man was a discontinuous producer of energy, but

the man of control is undulatory, in orbit, in a continuous network" (Deleuze, 1992, pp. 5–6). Control, then, does not discipline or mold, but mediates the circulation of social actors, such as humans, information or computers, through a continuous network.

Two examples elaborate Deleuze's theory of control. Guins (2009) cites Deleuze's own example of control as a highway system. "People can drive indefinitely and 'freely' without being at all confined yet while still being perfectly controlled," Deleuze suggests (Quoted in Guins, 2009, p. 6). Freedom like the open road, according to Guins in his review of Deleuzian control, is "a practice produced by control" (2009, p. 7). The freedom to communicate depends on forms of control in a medium. Though Guins offers the highway as a model of control, fixed roads seems a strange metaphor for a dynamic modulation. Brian Massumi, in contrast, interprets control as a "transitive mode of power" that facilitates circulation. Transitivity has capacities related to the passage or duration of a signal in a medium (2002a, p. 86). He writes on capitalism and control that, "[p]resent-day capital is the capillary network of the capillary, the circulator of the circulation, the motor of transitivity" (2002, p. 88). Capital, like the highway system, facilitates circulation in society through capital itself (money) that defines relations and exchanges. Roads do not modulate like the 'coils of the serpent' of capitalism. Massumi continues, "control is a modulation made a power factor (its flow factor). It is the powering-up–or powering-away– of potential. The ultimate capture is ... the movement of the event itself" (2002a, p. 88). Massumi suggests capitalism modulates how it links various potentials or events with the global market. Powering-up of potential appears as different modes of transitivity for events in how it moves an event through circuits of capitalism. Transmissive control is a direct response to this transitive control. These two examples offer a sense of control as being malleable and adaptive, all the while keeping circulation within set limits.

Deleuzian control also places a strong emphasis on time. Deleuze demarcates discipline from control through their changing temporalities. As he writes, "Paul Virilio also is continually analyzing the ultrarapid forms of free-floating control that replaced the old disciplines operating in the time frame of a closed system" (1992, p. 4). The factory illustrates how control can be characterized by how its modulations change over time (see Lazzarato, 2006). Factories not only discipline the worker through intense surveillance and social conditioning to optimize their labour output, but also control the workers through modulating performance bonuses that adapt to the variable inputs of labour and ensure maximum productivity. These forms of control appear much more dynamic than those imagined by Beniger and the focus on the temporality of control remains well suited for instant and changing operation of digital systems. Transmissive control has a deep debt to this emphasis on the temporality of control by Deleuze.

Despite this introduction to communication and control, the literature remains broad. As a result, the concept of transmissive control focuses on two key aspects of the literature of communication and control: technology and time. Media depend on technologies that express certain temporalities. In order to address the variety of approaches to these themes the review bifurcates into two nebulous fields: mechanisms of Internet control and perspectives characterizing the current epoch of time. Approaches to time and media remain broad and predominately cultural in focus, whereas mechanisms of control focus on the actual technologies supporting control. The review begins with the former to allow the power of temporal control to be clear when discussing the actual mechanisms that manifest it. This dissertation situates itself within these two lines of research.

Mechanisms of Control

Many approaches to the mechanisms of digital control describe it as a process akin to the enclosure of the commons (Andrejevic, 2002; Bettig, 1997; Dyer-Witheford, 2002). The digital enclosure refers to how copyright holders, Internet Service Providers and software firms fund the development of digital locks and exclusionary technologies to prevent unauthorized usage of digital networks (Dyer-Witheford, 2002, pp. 132–135) and to channel users into streams that deliver profiled advertising, produce cybernetic commodities based on a user's web usage and consolidate web traffic into commercial web portals (Dahlberg, 2005, pp. 163–172). The digital enclosure, in effect, entrenches "economic and political interests" through "the systematic incorporation of technological choices in absence of consumer choices" (Elmer, 2004, p. 26). Space dominates the theories of enclosure that function to create secure spaces and restrict access to insecure spaces.

The spatial bias of the digital enclosure has proven problematic given the rise of advanced traffic management software. With the advent of web 2.0, control shifts from the enclosed spatial movements of enclosures in favour of digital control during transmission. As Richard Rogers writes, research must "move beyond the dominant treatment of the Web as a set of discrete sites, which are blocked or accessible" toward the web "as an information-circulation space" (2009a, p. 229). The binary, at its worst, threatens to reduce the complex ramifications of advance traffic management software into a question of good (open) and bad (closed). Further, the spatial metaphor of enclosure describes the problem as a fixed and static system. Software does not operate as a structure, but as a process. Communication does not exist permanently outside the influence of control, but temporally. The case of The Pirate Bay illustrates how resistance involves a race. Pirates race to find the virtual limits of control as quickly as control technologies modulate their operation to encompass resistance. While the broader

political economy of the digital enclosure remains useful, transmissive control adds a more precise account of the struggle online that avoids the confines of a simple concept of open and closed and the limits of space and structure.

In contrast to the historical metaphor of enclosure, Alexander Galloway (2004), in collaboration with Eugene Thacker (2004, 2007), draws upon the work of Foucault and Deleuze to develop the concept of the protocol. It describes how control operates in decentralized computer networks. Protocols are,

> a totalizing control apparatus that guides both the technical and political formation of computer networks, biological systems and other media. Put simply, protocols are all the conventional rules and standards that govern relationships within networks. (Galloway & Thacker, 2004, p. 8)

Protocols function as an apparatus binding together nodes, humans and code in a decentralized network. Control manifests through protocols distributed among the heterogeneous nodes of a network. To join a network, nodes must obey the rules of a protocol. By defining the rules of networking, protocols maintain control in decentralized networks. Without abiding by the rules of a protocol, a node cannot join a network. Protocols create networks where control is immanent.

Protocols form networks with multiple topologies – legal, technical, economic and social ones. Protocological control fixes topological configurations according to certain logics of centralization or decentralization, political or technical. Networks develop as a result of these topological relations. Galloway and Thacker provide a vital link between the development of networks and the work of Deleuze and Simondon in order to conceptualize how networks morph and form and most importantly how this individuation has a politics – in fixing relations – beyond any moment of connection and interconnection (cf. Parikka, 2010, chap. 3).

Problematically, their insight does not deliver past theoretical comparison. Individuation notably would depend on certain topologies overriding others, yet they offer no explanation of this struggle. Consider the multiple topologies manifested, at least technically, from the Internet being a set of multiple protocols. The Internet is defined by the Internet Protocol Suite (TCP/IP) that contains a Transmission Control Protocol and an Internet Protocol, as well numerous nested application protocols. Though Galloway and Thacker acknowledge that, "a network is, in a sense, something that holds a tension with itself – a grouping of differences that is unified" (2004, p. 22), they do not push toward any greater theorization of the resolution or every politics of these tensions. If the network contains multiple topologies, how do they conflict or relate? If they all get along, then what are the stakes?

Robert Latham offers a more robust explanation of network formation through this discussion of the growth of the Internet. TCP/IP, throughout its spread, faced steep competition from other processes of internetworking, such as the Open Systems Interconnection (OSI) model (Latham, 2005; also see Russell, 2006). 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" (2005, p. 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, p. 149). He refers to these logics as the relations among networks or *network relations*. They emphasize how networking is a process of interconnection, 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. As a corrective to Galloway and Thacker, network relations point

toward an investigation of the various standards, software and protocols that include logics of connection with centrifugal and centripetal tendencies that congregate in central nodes or capitals of power (cf. Mulgan, 1991, pp. 54–55). Latham offers a new equation of network value (value = number of users x information) to suggest more strategic reasons for the formation of networks than simply the circulation of protocols. As will be seen, this approach leads to a more systematic discussion of the logics of networks, but it requires attention to the mechanisms actualizing network relations.

Protocols have also become less prominent on the web as a result of the rise of social media. Advances in web programming languages and browsers (known as Web 2.0) allow websites to behave more like software and have created sites know as social media platforms (Gillespie, 2010; Langlois, Elmer, McKelvey, & Devereaux, 2009; Langlois, McKelvey, Elmer, & Werbin, 2009; McKelvey, 2011; van Dijck, 2009). Web platforms, like Facebook and Twitter, behave much more dynamically than how Galloway describes protocols. 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). Platforms are a "convergence of different technical systems, protocols and networks that enable specific user practices and connect users in different and particular ways" (Langlois, Elmer, et al., 2009, p. 419). They are their own kind of networks that Lash describes as lifted-out spaces that admit actors to "participate in various forms of technological life" (2002, p. 24). Lifting out deliberately selects or filters some inputs, while filtering out others. Langlois, McKelvey,et al. (2009) highlight software as a key component of the platform that requires approaches drawing on software studies (see Fuller, 2008b). The rise of social media shift away from proctological control toward software control. Control becomes a dynamic result from software, rather than a static agreement networking decentralized nodes.

Raiford Guins (2009) identifies simple software logics functioning in 'device control', permeating society, particularly the household. These devices offer a variety of techniques of control; they "block, filter, sanitize, clean and patch" digital information to allow open circulation while embedding certain limits within this freedom. Guins focuses on the developments in media technologies that facilitate a 'control at a distance'. Control embeds in DVD players, televisions and computer games that can manage the circulation of content on the fly. If TCP/IP iconifies Galloway's concept of control, then the V-Chip System installed in television exemplifies what Guins calls *third generation machines of control*. The US congress legislated the V-Chip to be built into televisions so parents could block certain channels with a mature rating from appearing before their children. Blocking channels depends on software reading flags attached to a cable signal, checking its settings programmed by parents and blocks the relevant channel. Guins offers a promising start to a study of software as a mechanism of control. Since he draws most of his cases from film and television, he primarily focuses on the distribution of content, rather than its participation within a system of communication. Future projects then must extend his introduction of software and control to more complex interactive media.

Tarleton Gillespie (2007) raises an important aspect of the probabilistic aspect of control in his discussion of digital rights management. Intellectual property such as music or videos have always struggled with being copying, taped or bootlegged. The challenge is their media of transmission include unintended uses. Copyright, Gillespie nicely formulates, struggles "how to control the way that someone uses something that is freely handed to them" (2007, p. 652). Where copyright law has long attempted to regulate the uses of transmission media, he notes that digital rights management (DRM) strategies have risen as another means to embed restrictions of use within the technology itself. DVD players include the CSS DRM that pre-

vents *unauthorized duplication*. CSS among other control technologies also mentioned by Guins seek to *effectively frustrate* any unwanted usage. Effective frustration is a technique of control in part because it depends on a probabilistic model of user agency. As Gillespie writes,

> What is at stake here is not only a user's ability to act with a tool and on that tool, but also the user's perception of their ability and right to do so. To frustrate people's agency is less politically problematic than to convince them that they have no such agency to be frustrated. (2006a, p. 661)

Effective frustration presupposes a user agency that might go in unwanted directions and seeks to prevent these uses. When Gillespie sometimes slips from the nuance of discouraging uses to a more deterministic forbidding, his variance suggests a tension when discussing control. Although its more tangible to speak of its determination of usages, control has a probabilistic influence that includes its own limit. Effective frustration suggests a probabilistic control that acknowledges the possibility of uses out of control and purposely influences activity toward its intended uses. Techniques like digital rights management or others listed by Guins fit within what Karaganis (2007) calls an *ecology of control* that includes filtering software, Digital Rights Management and Trusted Computing. How might communication networks fit with this ecology?

Wireless networks prove just the medium to investigate the complex operations of control through software or more accurately, algorithms. Adrian Mackenzie in his investigation focuses on these specific bits and functions of code to transmit information amidst interference and physical obstacles. Wireless Internet is "an algorithmic mosaic of calculations carried out to allow communication to occur in the presence of many others" (Mackenzie, 2010, p. 68). Algorithms provide the technical mechanisms for a cultural affect that Mackenzie calls *wirelessness*. He writes,

> wirelessness designates an experience toward entanglements with things, objects, gadgets, infrastructures and services and imbued with indistinct sensations and practices of network-associated change. Wirelessness affects how people arrive, depart and inhabit places, how they relate to others and indeed, how they embody change. (2010, p.5)

Wireless networks, according to Mackenzie, are a kind of becoming of people and things with specific relations to spaces and times. Algorithms function to provide moments of connection and synchronization. Wirelessness stabilizes into momentary networks. Despite the seeming relation to the concept of control, Mackenzie argues that wirelessness brings "something irreducible to systems of control" (2010, p.213). Wireless networks never stabilize enough to enact control and to reduce one to the other would ignore the nuances of wirelessness.

Mackenzie offers the most developed approach to mechanisms of control through his discussion of the algorithm. In doing so, he aligns with an emerging trend in the study of the algorithms as processes of control (D. Beer, 2009; Galloway, 2006; Graham, 2005; Lash, 2007). Algorithms appear in the reappraisal of cultural studies by Lash. His reappraisal shifts emphasis from hegemony and its tendency toward epistemology to a post-hegemonic age with an emphasis on ontology. The study of ontology in a "society of pervasive media and ubiquitous coding" should focus on "algorithmic or *generative* rules" that are "virtuals that generate a whole variety of actuals" (2007, p. 71). Virtuality and actuality according to Lash corresponds with Negri's bifurcation of power into *potestas* and *potentia*. The former designates potential or raw power, such as bio-power or labour power, where the latter refers to its actualized power commonly associated with *power over* in a hegemonic sense. Potestas in a post-hegemonic environment emanates from generative rules, like algorithms, that have power precisely because they generate kinds of potestas. Algorithms constitute actualities of

postestas from the virtualities of potentia. In a way, wirelessness is a kind of potestas emerging from algorithms embedded in wireless routers that order the potentia of entanglements.

Where Mackenzie rightly points out the instability of wireless networks, wired networks are actually much more stable. Behind every router is a wired network whose algorithms exert considerable control over the transmission of information on the Internet. This dissertation then moves into the infrastructure behind wireless. Even though transmissive control operates on both wired and wireless networks, the nature of wireless radio modulations muddles the specific intentionality of control. Future studies could apply transmissive control to discuss its particular implications to wireless transmission and wirelessness.

Few sources in Internet studies address the matter of time and control. Although there is ample research on the World Wide Web and collective memory, most of these works focus on the act of remembering without dwelling on the theoretical questions of time and control (Ashuri, 2012; Garde-Hansen, Hoskins, & Reading, 2009; Mayer-Schonberger, 2011; Strangelove, 2005). Hellsten, Leyesdorff and Wouters (2006; 2004) argue search engines control remembering by recording websites at set frequencies and archiving only particular information. "Search engines," Hellsten, Leyesdorff and Wouters write "can be appreciated as the clocks of the internet, ticking at different frequencies and possibly leading to multiple presents" (2004, p. 919). These multiple presents conflict with search engines providing alternative histories and presents to its users. These studies offer a direction to study the technologies of control, but another literature needs to be explored to explain the times of control or how these processes function systematically.

Times of Control

Time is a "neglected area of internet scholarship" (Leong, Mitew, Celletti, & Pearson, 2009, p. 1282). Given this lack of a clear literature on Internet and time, this dissertation adopts a broader perspective of the relationship between technology and time. Numerous perspectives have attempted to describe the current temporal conditions and how these conditions endure through practices or technologies. A few in-depth reviews do exist on approaches to time and society by Adams (1990, 2006), Abbott (2001), May and Thrift (2001), Brose (2004) and Hörning, Ahrens and Gerhard (1999). These approaches include questions about democracy and time (Connolly, 2002; Rosa, 2003; Scheuerman, 2004; Wolin, 1997), geography (May & Thrift, 2001), sociology (Adam, 1990; Castells, 1996), media studies (Hassan & Purser, 2007), queer theory (Dinshaw et al., 2007; Freeman, 2010) and science and technology studies (Edwards, 2003; Wajcman, 2008). Scheurman and Rosa (2008) offer a good history of the theories of time, specifically accelerating time, that could use more in depth discussion. Gaston Bachelard (2000, 2008), Walter Benjamin (1969), Henri Bergson (1988), Gilles Deleuze (1989, 1994), Norbert Elias (1992), Martin Heidegger (1962, 1977) and Henri Lefebvre (2004) all appear within these approaches.

Three major approaches appear in the specific literature probing the contemporary temporal condition. First, technology participates in a culture of speed where time moves fast. Manuel Castells and Paul Virilio offer two major approaches in this area. Concepts of high-speed and fast relate to a second literature focused on the acceleration of society. Technology is one major force in this general *acceleration* of society that causes a lack of time and a problem for political time. William E. Scheurman and Hartmut Rosa appear prominently in this area. Finally, time has been cited as a matter of scarcity and a growing literature considers this scarcity as a kind of *attention economy*. These three approaches situate the ensuring discussion

of transmissive control and temporal economies; however, before drawing the section to a close, a few nebulous sources drawing on political economy will be introduced. These sources provide the closest counterparts to temporal economies.

No figure looms over the literature on time and society more than Paul Virilio (1995, 2004, 2006). His work, controversial and debated, continues to provoke discussion about speed in modern society (see Armitage & Roberts, 2002a). His central contributions remain a theory of speed and its social ramifications. Dromology is his concept to "study the logic of speed" (Armitage & Graham, 2001, p. 112). Speed is a general phenomena in the work of Virilio that he argues has become the central logic of modern society. According to Virilio, "speed is time saved in the most absolute sense of the word, since it becomes human time" (Virilio, 2006, p. 46). Speed then is power and the stratification of speed creates class. Speed produces class (Crogan, 1999, p. 144). Forms of incarceration like the poorhouse, a prison or the shantytowns "solve a problem less of enclosure or exclusion than of traffic. All of them are uncertain places because they are situated between two speeds of transit, acting as brakes against the acceleration of penetration" (Virilio, 2006, p. 33). Prisons presumably move slow, where highways and private boulevards afford faster forms of circulation. These two different speeds of transit appear akin to the stratification of society into classes though he never actively describes the forms of hierarchy in depth.

Cyberspace is another focus in dromology (Virilio, 1995, chap. 7). It is an essential part of dromology because "information is only of value if it is delivered fast" (1995, p. 140). Armitage and Graham (2001) build on this observation in their suggestion of 'dromoeconomics': as a political economy of speed. Modern or rather *hypermodern* capitalism depends on the Internet to negate time so it can function at the global stage. Armitrage and Graham write, "the overproduction of speed is the *negation of time*; it is the *consumption and destruction of time* rather

than its emancipation" (2001, p. 118). Capitalism depends on speeds for its global economic transactions. Armitage, now collaborating with Roberts (2002b), argues that the business literature around the millennium embraced high speed as a kind of *chronotopism*. Certainly, high-speed came to be valued and celebrated with the rise of the Internet. Here within the work of Virilio, speed makes time irrelevant. High-speed allows the time usually taken in movement to be ignored. Greater control over velocity creates new opportunities, new values, that drive invest in technology.

Speed, in Virilio, is a problematic concept due to its singularity and its relation to space. Discussing Internet time as speed reduces the complexities of network duration to its movement through the network. Massumi introduces the paradox of the arrow by Zeno of Elea who questions the nature of an arrow in flight. The flight of the arrow cannot be reduced to spatial positions, but must be understood as a trajectory over time (2002a, pp. 5–6). Thinking deeply about time – an approach since Bergson – requires a meditation on its nature without reducing it to movement and speed. What is speed other than the time it takes to travel through space? How else can this travel or transmission be understood? Speed also appears as overly constrictive in its singularity in Virilio's formulation. Crogan distinguishes between the work of Virilio from Deleuze and Guattari. Though clearly indebted to the work of Virilio, Deleuze and Guattari question how he assimilates three distinct speeds (nomadic, regulated and speed of nuclear proliferation) into one "fascist" character of speed. They argue in favour of the multiplicity of speeds, rather than overall tendency of speed (1999, pp. 141–143). Both these criticisms illustrate some clear shortcomings in the work of Virilio and point toward a more sustained reflection on time and the politics of its multiplicity.

Castells offers a more nuanced approach to the *high-speed* or more accurately *instant* nature of information and communication technologies and how they induce temporalities. Com-

munication, according to Castells, is a central mechanism in the production of 'flows': "the purposeful, repetitive, programmable sequences of exchange and interaction between physically disjointed positions held by social actors in the economic, political and symbolic structures of society" (Castells, 1996, p. 412). These flows define societies and economies. Digital communications allow for rapid or instant flows across the world. *Instant exchange*, according to Castells, creates a global *simultaneity* that conquers barriers between time, such as distance. A global world, in other words, mixes all regional times together. Mixing times "creates a temporal collage, where not only genres are mixed, but their timing becomes synchronous in a flat horizon, with no beginning, no end, no sequence" (Castells, 1996, p. 462). Time evaporates into an instant, on-demand network. Castells calls this *timeless time* that he describes through Lebinizian definition of time as "the order succession of 'things', so that without 'things' there will be no time". Time naturally appears to humans in a sequence, but timeless time "systemically perturbs" a "sequential order" through time-compression, instantaneity or discontinuity (1996, p. 464). Access to timeless times *belongs* to the certain concentrations of flows with material supports that Castells defines as the *space of flows* (1996, pp. 410-418). Global elites participate in timeless time through their organization in the space of flows. Their placement affords them power to control the distribution and domination of sequences that conflict with other biological times and local times or "socially determined sequencing" (1996, pp. 464-468).

Though Castells offers a strong analysis of timeless time as the central characteristics of modern societies, his argument must be situated in his larger work where "the dominant trend in our society displays the historical revenge of space, structuring temporality in different, even contradictory logics according to spatial dynamics" (1996, p 467). Despite the promises of a network of *temporal collage*, he reduces time to a matter of the space – often with the

hope these regions might resist the global timeless time. He chooses to dwell more on the *space of places* (as he puts it) then the complex manifold temporality of the *space of flows*. How timeless time alters or perturbs sequence remains unclear? How does *timeless time* seem unnatural compared to natural temporalities. What are the components of a sequence? How does un-ordering occur? Though sequence suggests a system of relation – perhaps between past, present and future – terms do not appear to cultivate a systematic approach.

If speed and timeless appears too monolithic, it could be in part do to the tendencies toward a kind of technological determinism in their literature (Wajcman, 2008, pp. 66–67). This criticism comes from another approach in the literature that focuses on the social dynamic of acceleration as a more systematic approach to speed (Hassan, 2009; Rosa, 2003; Rosa & Scheuerman, 2008; Scheuerman, 2001, 2004; Wajcman, 2008). Acceleration refers to a loss or decline of the amount of time for perception and decision. Less tangible units of time are needed for decision or change. Acceleration is a long-term and historic process distinct – though related – to economic change (i.e. capitalism) and non-economic factors. Most of the literature defines acceleration according into three types: technological acceleration, acceleration of social change and the acceleration of the pace of life (Rosa, 2003; Scheuerman, 2004; Wajcman, 2008). These three produce, according to Scheurman who in turn draws on Rosa, a "self-propelling feedback cycle" (2004, p. 18). Since these cycles of acceleration cause a loss, it provokes an anxiety that there is no longer time to think, deliberate or relax (Menzies, 2005; Rosenberg & Feldman, 2008; Wolin, 1997). Though Scheuerman acknowledges that concern over the fast pace dates back to as far as Montesqieu commenting on the hurry of France and Alex de Tocqueville's concerns over the restless American character (2004, pp. 5–6), the acceleration of certain social practices, notably trading, leads to a de-synchronization of those institutions that cannot *speed-up* (Rosa, 2003, pp. 25–28). Deliberative legislatures are too

"slow-going" to catch up with "high-speed" communication technologies (Scheuerman, 2004, p. xiii–xiv). Though this concern sounds similar to the work of Virilio, acceleration theory is quick to offer more concrete analysis and suggestions, such as reflexive law (see Scheuerman, 2004, chap. 6).

Information and communication technologies, particularly the Internet, participate in all three kinds of acceleration. The Internet in particular increases the pace of the first type of technological innovation. Scheuerman cites the launch of new products as one of example of this pace. High-speed communication also enables new forms of collaboration leading to changes in work habits and, by extension, accelerating social change of the workplace and the family. Finally, greater connectivity increases the pace of everyday life as human must process the greater volumes of information running through their daily circuits, as well as being connecting to a greater number of tasks and activities (2004, pp. 9–15). Despite an association with technology and speeding-up, the literature does not assign a determining element to technology. Approaches in science and technology studies emphasize the *interpretive flexibility* of new technologies that will always be mediated by social practices. The historical approach also recognizes that technologies co-exist, so change is not immediate, but brokered between different rates of adoption and affordances (Wajcman, 2008, pp. 66–67). In this way, technologies participate in a complex of "fast" and "lagging behind" (Scheuerman, 2004, p. 18). Wajcman suggests "rather than simply reading [new technologies] as adding to time pressure and accelerating the pace of life, mobile modalities maybe be creating novel time practices and transforming the quality of communication" (2008, p. 70). The call to question time practices, however, raises issue with the dichotomous approach in the literature between fast and slow. Though certainly less totalistic than Virilio or Castells, the emphasis on acceleration binds

analysis of temporal control to one of either accelerating or lagging behind. Is temporal control as simple a dynamic as acceleration or might a more complex taxonomy appear?

A final approach to temporal control might be found in a much earlier concept of the attention economy (Goldhaber, 1997; Lanham, 2006; Simon, 1971). If there is a perceived loss of time or an acceleration of time, then how might different temporal practices have a value over one another? Herbert Simon introduces the concept to discuss the consequences of "information-rich worlds" that have "a poverty of attention" (1971, pp. 40-41). Human cognition can only *attend* to so much. Although attention appears similar to a loss of time, Simon introduces the problem as a means to discuss the use of information technology to augment human limitations of information processing. Organizations only benefit from information technology if "it listens and thinks more than it speaks" (Simon, 1971, p. 42); in other words, computers only benefit organizations by intensifying information processing and consolidating information. Firms must calculate the comparative advantages in information processing between humans and machines when optimizing their systems to conserve scarce attention. Differences in attention capacities have an economic value, so buying a new computer system must be rationalized within a framework of attention economics. By offering this concept, Simon offers an approach to the problem of a lack of time for information processing or attention though a consideration of the relations of attentions in an organization. Underlying his claim is a sense that time – chiefly saving time and thereby attention – has an economic value.

Audiences studies or studies of spectatorship have long recognized the value of attention (Beller, 2006; Crary, 2001; Smythe, 1981). Smythe (1981) offers perhaps the clearest distillation of the value of attention in his concept of the *audience commodity*. Audience commodities are packaged and sold as sets of attention tied to specific demographics. Broadcast television is an attention economy because the industry produces and sells blocks of attention to its advert-

isers. Programming seeks to create revenue for its producers by capturing blocks of scarce attention. Studies of YouTube continue this lineage by questioning how the video sharing platform also functions as an attention economy. Shifman (2011) discusses attention economies in relation to views on YouTube. Popular videos have different modes of capturing the attention of their audiences. Two appear but relates the concept to two popular theories of popularity online: Memes and virality are two such modes. Both adapt biological concepts to explain the circulation of content and the capture of attention. Biologist Richard Dawkins (1976) coined the word memes to describe "small cultural units of transmission, analogous to genes, which are spread by copying or imitation" (Shifman, 2011, p. 188). Videos on YouTube capture attention either virally "as a clip that spreads to the masses via digital word-of-mouth mechanisms *without significant change*" or mimetically that "that *lures extensive creative user engagement* in the form of parody, pastiche, mash-ups or other derivative work"(Shifman, 2011, p. 190). Both these terms capture the attention of its viewers, but they have distinct modes of attending either as watching or as manipulating and remixing. Re-mixes and mash-ups of memes suggest that the audience commodity has shifted from simply synchronized viewing to aggregating participation. These two approaches point toward the multiple ways to create a common attention – an audience – that have a value.Attention economies lend themselves to a broader discussion of the political economy of time. Capturing attention – a block of synchronized viewing – is just one crystallization of temporality that oscillates between a product of a socio-technical assemblage and a unit of value in an economic market. What other temporal economics might be possible?

An emerging literature has begun to question the multiplicity of times and values that participate as a kind of political economy. Though Artmitage and Graham (2001) do hint at linking speed with economies, their dependence on Virilio narrows their perspective on the mul-

tiplicity of temporalities. Leong, Mitew, Celletti and Pearson (2009) provide an excellent theoretical review of the approaches to time of the Internet. They offer "a comparative tool-kit of temporal conceptualizations for internet researchers looking to develop new methodologies for studying network temporalities" (2009, p. 1282). Even though their approach offers a strong framework that informs the Theoretical Framework section in this chapter, they do not address the politics of multiple times. How do the multiplicity of temporalities compare or conflict? Sharma (2011) works toward a "bio-political economy of time" through the concept of "power-chronography". It is an antidote to the reactiveness of speed theory or any of the singular approaches to time discussed above. The approach "is concerned with the multiplicity of time, the interdependent and inequitable relations of temporal difference that are compressed deep within the social fabric" (2011, p. 66). Time is political regardless of its acceleration or speed. Even if society moves faster or slower, it has different ways of valuing and expressing time. Air travel, an example drawn from her work, involves both a faster pace that participates in the "constitution of time-scarcity by dominant institutions actively working to create new forms of social control – including the normalizing of overwork by making it more palpable" (Sharma, 2011, p. 73). First-class makes overwork luxurious. While Sharma focuses on a broader discussion of the production of temporalities, Hassan (2007) focuses specifically on the temporal control of the Internet being capable of a "connected asynchronicity" that replaces singular "clock time" with a multiplicity of times. Connected asynchronicity allows people to "have the capacity to create their own times and spaces" (2007, p. 51) and even though this claim might over reach the dominion of clock time as if it thwarted other times, connected asynchronicity does lead to questions about how new times might be created with their own particular economic values. How might it create new synchronizations – like syn-

chronizations of attention – that have economic value? These approaches point toward a political economy of Internet temporalities.

The literature above does offer a few lessons to cultivate these concepts. First, it emphasizes the hybridity of technical and social forces producing time as opposed to situating temporal control as socially constructed or technologically determined. Second, a clear shift appears in the literature from early concepts of singular time to more time complex versions where time is understood as being multiple and assembled. The approach of the dissertation, as will be developed, is one of the multiplicity of time and its expression. Finally, much of the reading of temporal control tends toward a hermeneutic tradition, mostly concerning the human. This dissertation diverges away from the hermeneutic approaches to time offered by most of these authors by focusing on how transmissive control is an algorithmic process.

This dissertation situates itself within communication studies and its study of control. In summary, this review emphasizes two sides of the time and control: mechanisms of control and the systems ensuing from these mechanisms. Transmissive control involves Internet routing algorithms as its mechanisms and asynchronicity as the ensuing system. The rest of the dissertation is dedicated to exploring these two components of transmissive control. To elaborate further, the following section begins this task by engaging with its theoretical assumptions.

Theoretical Framework

Transmissive control refers to a systematic usage of the conditions of transmission to produce and assign common times of communication. Unlike many of the approaches above, this dissertation argues that the Internet is an asynchronous communication system with multiple times resulting from multiple rates of transmission. Asynchronicity creates the conditions for

transmissive control to optimize and stratify the multiple times of the Internet. The following section outlines a theoretical framework to support this view of time, transmission and control. Its constituent elements are the concepts of expression, time and the assemblage as developed by Deleuze and Guattari. As will be discussed, these terms cooperate to explain a system of transmissive control on the Internet.

This dissertation considers transmission as a matter of *expression* (Deleuze & Guattari, 1987; Lazzarato, 2003; Massumi, 2002b). Expression refers to a central concept in the work of Deleuze and Guattari. They suggest language includes both content and expression. Content concerns *what* is said and expression concerns *how* it is said. The distinction offers a different way of stating 'to impart' – the word used by Raymond Williams to define communication at the start. Impart might refer to transferring knowledge about the hour as content or to transmitting a common moment of time as an act of expression. In other words, ringing bells include the hour as the content, but also includes an expression in the form of reverberating sound waves. Studying expression focuses on the conditions internal to the way the world comes to be through language, not its semantic content.

Expression correlates with how communication media transmit signals. As Ian Angus writes, the work of Harold Innis "gives the discursive turn in the human sciences another twist. The turn toward language is expanded into the notion of media of communication as a theory of expressive forms and then analyzed from the viewpoint of the materiality of forms of expression" (Angus, 1998, np.). Media, in other words, include not only the message, but also its expression through materials. Where Innis focused on this expression through the physical properties of clay and stone, it is now algorithms that set the conditions of expression on the Internet. Information on the Internet – its processes, mutations, syntheses and repetitions – must be transmitted as packets by algorithms. Packet switching underlies the co-

existing and overlapping modalities of the Internet communication that include labour (Lazzarato, 1996; Terranova, 2004), deliberative dialogue (Dahlberg & Siapera, 2007; Poster, 2001) and ideological reproduction (Dean, 2008). Without algorithms routing packets, messages would not travel through the array of networks comprising the Internet. These examples illustrate the importance of transmission as expression, but how might the conditions of transmission itself be understood?

The limits and conditions of transmission concern time. Transmission involves time by connecting different humans or machines together in common moments of exchange and coordination. How much or little time does it take for there to be resonance between two people or machines? Who might be part of this common time? The matter of time, however, is not a matter of seconds or units of time. Time is multiple, an assemblage of different kinds of transmissive materials and communication systems (Leong et al., 2009). Gilles Deleuze (1990, 1994, 2004) offers a theoretical framework to unpack the asynchronicity of the Internet. He rejects a linear definition of time to suggest it is multiple and full of differences. His approach lends itself to transmissive control that produces and assigns rates of transmissions to create multiple times.

Deleuze appropriates concepts from the philosophies of Gilbert Simondon and Henri Bergson to elaborate his own philosophy of time (Atkinson, 2009; Toscano, 2009). Deleuze's philosophy of time first draws on Bergson and his concept of *duration* as an alternative formulation of time. Both Bergson and Deleuze use the analogy of a sugar cube to describe the concept. A sugar cube in water has both a spatial identity as a cube, but also a temporal identity as a cube dissolving. Its duration has to be understood as a series of differences between itself and past states of being less dissolved. As Deleuze writes about the sugar cube,

> it also has a duration, a rhythm of duration, a way of being in time that is at least partially revealed in the process of it dissolving and that how this sugar differs in kind not only from other things, but first and foremost from itself. This alteration, which is one with the essence or the substance of a thing, is what we grasp when we conceive of it in terms of Duration. (1990, p. 32)

All things – be they sugar cubes or humans – have a duration. Where Bergson focused on the human nature of duration, Cyberneticist Norbert Wiener suggested that duration could apply to machines – in his words "automatons" – as well (1948, p. 44). Whether human or machine, a duration is a synthesis of the past (less dissolved), a future (more dissolved) and a present (dissolving). Different beings have different durations synthesizing these three. Deleuze extended the concept of duration as part of his general philosophy of time. Everything – person or thing – has a *becoming*: Deleuze's version of duration (A. Parr, 2005). Becomings do not follow a singular order as found in the natural sciences and its approach to time. James Williams writes "processes make times and those processes are determined by singularities rather than be regular features adapted to general laws and relations" (2011, p. 4). Deleuze stresses that time is multiple, a synthesis of past, present and future (see Ansell-Pearson, 2002; J. Williams, 2011). Deleuze extends Bergson by theorizing becoming as a processes that can be common among beings unlike the singularity of duration.

Deleuze's collective aspect of becoming draws on the work of Gilbert Simondon (1992, 2009a, 2009b). Simondon calls his approach *ontogenesis* to emphasis the difference from philosophical ontology. Adrian Mackenzie, one of the first media theorist to draw on the work on Simondon, succinctly noted the difference: "ontogenesis (that is, how something comes to be) rather than ontology (that is, on what something is)" (2002, p. 17). Theoretical focus, as a result, shifts concepts like *individuals* to *individuations*. While this concept at first appears like

duration, ontogenesis can occur between multiple individuations. A system with many individuations has, according to Simondon, a *metastability*. The concept describes "the notions of order, potential energy in a system and the notion of an increase in entropy" (2009a, p. 6). Metastability encapsulates the tensions and relations between individuations. As Deleuze writes in his short commentary on Simondon, "a metastable system thus implies a fundamental difference, like a state of dissymmetry. It is nonetheless a system insofar as the difference therein is like potential energy, like a difference of potential distributed within certain limits" (2004, p. 87). Metastability leads to the process of *trans-individuation* where multiple individuations occur in common. Deleuze refers to the same process as a *collective becoming* – one becoming common to all. Crucially, Deleuze refers to control societies as having a "perpetual metastability" echoing how Communication Studies defines control as internal social organization (1992, p. 4). Metastability involves collective becomings in social life. The work of Deleuze on time then offers a beginning to an understanding of the power to create order during collective becoming.

The conditions of metastability and control depend on the concept of *assemblage*. Deleuze in his collaborative work with Félix Guattari use the term to refer to a unit of metastability or collective becoming. The Internet operates and functions as a heterogeneous set of becomings theorized by the concept of an assemblage. This concept draws out the metastability of the Internet as well as illustrates the important function of control to be discussed later. Assemblage is the English translation of the French verb <<*agencement*>> "usually translated as 'putting together', 'arrangement', 'laying out', 'layout' or 'fitting'" (Wise, 2005, p. 91). The noun captures the variety of the original French, but not the processual nature of assembling. Assemblage refers to not just the outcome, but a "process of arranging organizing and fitting together" to create "a whole of some sort that expresses some identity and claims a territory"

(Wise, 1997, p. 77). Assemblages also stress the interplay between technologies and humans since the term deliberately avoids specifying what its components could be. As Deleuze states "machines don't explain anything, you have to analyze the collective arrangements of which the machines are just one component" (1995a, p. 175).

Assemblages have a direct relationship to time because their components exist in metastability that produces collective becomings. Lazzarato, drawing on the work of Deleuze and Bergson, elaborates on how technologies as assemblages relate to time. He remarks "electronic and digital technologies operate like the material and spiritual syntheses in Bergson: *they crystallize time*" (2007, p. 110). Where Bergson would speak of crystallization through human existence (the material synthesis), Lazzarato suggests technologies participate in the crystallization of time in that they fix certain relations of past, future and present. Technologies *as* assemblages create certain temporal systems of resonance. Communication is one form of resonance in an assemblage that crystallizes becomings. Forms of transmission express resonance between components of an assemblage. Crystallizations of collective becomings will be referred to as *temporalities*; they involved shared past, presents and futures as well as conditions of metastability. These crystallizations arise when a communication system involves a systematic usage of transmission to control its metastability. Transmissive control involves the coordination of expression – either deliberate or a property of the medium itself – to create temporalities. This control is not imposed on the assemblage, but immanent in its conditions of transmission.

Deleuze and Guattari offer a series of questions and concepts of an assemblage and these components also apply to a discussion of temporality and transmissive control:

1. What is the content of an assemblage? What humans and non-humans fit together during its existence? They offer the concept of a *machinic assemblage* "of bodies, of

actions and passions, an intermingling on bodies reacting to one another" to discuss the components of an assemblage (Deleuze & Guattari, 1987, p. 88). The content in this dissertation refers to the components of temporality that include humans, machines, wires and all other becomings.

2. How do the contents of an assemblage act collectively? How does an assemblage act in concert with or under control? Deleuze & Guattari refer to systems of language and communication as an *assemblage of enunciation* "of acts and statements, of incorporeal transformations attributed to bodies" (Deleuze & Guattari, 1987, p. 88). This concept offers a way to systematically think about the resonance and metastability of an assemblage resulting from communication. Communication – by linking becomings together parts of an assemblage – functions as a collective *assemblage of enunciation.*
3. How does an assemblage have *territorial sides* that "stabilize it" (Deleuze & Guattari, 1987, p. 88)? How does an assemblage have *cutting edges of deterritorialization* "which carries it away" (Deleuze & Guattari, 1987, p. 88). These latter two concepts will be discussed further on in this section, but in general refer to the crystallization or stability of the assemblage. These concepts focus on the trajectory of the Internet that will help define transmissive control and its limits.

Assemblages involve both a machinic assemblage of bodies, namely those parts of a communication system, and a collective assemblage of enunciation, namely how a communication system expresses these components together in a common temporality. This dissertation emphasizes the collective assemblage of enunciation as a way to explain how transmission functions systematically to produce temporalities.

The collective assemblage of enunciation is a way to understand how transmissive control functions systematically. A language is the most obvious example of an assemblage of enunci-

ation. A word can be said to express when it has a connection to the outside world. Deleuze and Guattari refer to these as *order words.* They define the concept as "designat[ing] this instantaneous relation between statements and the incorporeal transformations or non-corporeal attributes they express" (1987, p. 81). They continue,

> Anyone can shout, "I declare a general mobilization," but in the absence of an effectuated variable giving that person the right to make such a statement, it is an act of puerility or insanity, not an act on enunciation. (1987, p. 82)

An order word refers to an "instantaneous relation" between a statement and its effect in the world. While this example of language as a collective assemblage of enunciation might be helpful, it still does not fully explain how Internet packet switching might function as such a system. Deleuze laters offers a discussion of the order-word in relation to control without the emphasis on language. His discussion implies that the collective assemblage of enunciation involves both information or "the controlled system of order-words that are used in a given society" (1998a, p. 18) and communication or the "transmission and the propagation of a piece of information" (Deleuze, 1998a, p. 17). Where information to Deleuze refers to the commands of a ship, transmission concerns the range of the human voice as the crew shouts at one another. Where a shouted command might have an "instantaneous relation" between language and the outside, a communication system like the Internet has a more complex temporality resulting from its unique mode of transmission. Just as the range of the human voice creates an order to human organization on a ship, the nature of Internet transmission has its own influence on social organization. The collective assemblage of enunciation then offers a way of talking not only of information as orders, but also control through transmissive control.

Although the Internet certainly contains a controlled system of order words, the larger question remains its power of transmission. Certainly packets function as order words as they cause a reaction in another computer on the same network. A request for an HTTP session includes a variable of expression to establish an HTTP session. So much of Internet traffic functions as order-words: packets trigger algorithms, prompt a friend to chat, warn a customer of a scam or warn a usage capacity has been exceeded. Given the broad distribution of information, the object of study shifts from order words to how they are transmitted or communicated. Rather than focus on the system of information in a Deleuzian sense, a richer understanding of an assemblage comes from understanding how it transmits information systematically – a question of transmissive control.

Transmissive control refers to how transmission functions systematically to produce and assign temporalities. It is a kind of collective assemblage of enunciation for expressing time through patterns of transmission. Massumi suggests control is a 'transitive mode of power' (Massumi, 2002a, p. 86). Questioning transmission control requires an investigation into the *regime* of passage or "what effects it lets pass, according to what criteria, at what rate and to what effect" (Massumi, 2002a, p. 85). Regime is a key word as it seeks to describe the systematic function of transmission rather than specific moments. Various transmissions with rates to passage become repeatable patterns with common pasts, presents and futures. It does not control time, but expresses temporalities which contain forms of control.

In a way, transmissive control *as* collective assemblage of enunciation resembles Bergson's description of the human brain. The brain is a system of communication that he likens to a "central telephone exchange" that communicates messages to different parts of the body (1988, p. 30). Without overwhelming the analogy with a discussion of Bergson's theory of consiousness, his sense of a telephone exchange involves the expression of action in society. An

exchange coordinates actions between different organs. As Lazzarato writes, "the brain is just an interface, in the sense that it translates one speed into another, one movement into another; an interface that translates the infinite flow in accordance with the needs of our action. It is a 'commutator' between different degrees of the real" (Lazzarato, 2007, p. 99). Without this "communicator" and its capacities for control, actions would not occur. The example of Bergson's telephone exchange offers a glimpse into how transmissive control functions systematically. This systematic function, however, is more complex due to the particular conditions of transmission on the Internet.

The transmissive control of the Internet *modulates* – a general concept in the work of Foucault (1978) and Deleuze (1988, 1992) describing transformation and malleability. Though Deleuze argues modulation distinguishes societies of control from disciplinary societies, Foucault introduces "temporal modulation" to describe penalties in the prison system indicative of a disciplinary society (1978, p. 107). This seeming contradiction demonstrates that modulation, far from being some specific trait of societies of control, varies itself depending on its usages. Often modulation refers to a form, but both Foucault and Deleuze refer to modulation in relation to time. Deleuze, for example, imagines

> a city where one would be able to leave one's apartment, one's street, one's neighborhood, thanks to one's (dividual) electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position – licit or illicit – and effects a universal modulation. (1992, p. 7)

What matters in this allusion is the computer synchronizing a person and their urban environment in real-time to control their movements. Computerized control creates a *universal modulation* between all the barriers in the city, one that changes and adapts to a person's

movement. Internet transmission modulates by being a dynamic and multiple synthesis of past, present and future. Packets experience specific transmissions depending on algorithms integrating past and future at the moment of transmission. Patterns in transmission create different temporalities online that can be distinguished by their speed, quantification of time (i.e. clock time), allocations of time (i.e. windows of time), synchronization and frequency. Internet transmissive control modulates to produce and assign a multiplicity of temporalities.

This dissertation introduces the concept of the *temporal economy* to explore how transmissive control creates value. A temporal economy refers either to a temporality with a particular order in its metastability that has a value or a system of temporalities that have their own specific values as well as a relative system of value. Either way the concept stresses that temporalities have a value akin to an economy. Telegraphy, for example, could deliver a message before the arrival of a train. A control message could arrive before a train; it prevented trains from arriving at the same time to cause an accident. The telegraph created a temporal economy that had value by synchronizing its operations between geographically disperse stations and moving trains (Beniger, 1986, pp. 226-237).

The Internet differs from other temporal economies because of its capacity for *asynchronous communication* that allows for multiple temporalities simultaneously. Most temporal economies create value by *synchronizing* the assemblage. The word itself offers an indication of temporality. It combines the Greek *syn* meaning "united or connected together" and with Greek word *khronos* for "time". Generally synchronous refers to a communication system that would offer a common temporality to its participants. Chapter Two in particular offers a history of the kinds of temporalities associated with communication systems before the Internet. The Internet, on the other hand, is asynchronous. Allon (2004) explores a comparative system through a description of the smart home. Control manages an occupant's time and movement

as "strategies of control utilize... both modalities of time and the distribution of temporalities." The smart home as "the public/private workspace" and the "exploitation and order of bodies" occurs through "the control of time (work-time/private time), rather than spatial separation" (Allon, 2004, p. 269). The smart home, as a space managed by computers, involves a multiplicity of different times or *asynchronicities.*

Advances in Internet traffic management algorithms attempt to supersede asynchronous communication with a *poly-chronous* one. Internet Service Providers and other network owners have come to see Internet transmission as out of control. Their networks cannot support the diversity and amount of temporalities produced by asynchronous communications. As a result they have begun to prune and manage transmission to create a stratified network of temporalities. *World of Warcraft,* as discussed, fell into one such temporality on the Rogers network. Its users became out of synch with their fellow players. This is just one example of many tiers being developed by Rogers. Their efforts illustrate how bandwidth management techniques reduce certain kinds of transmission. Transmissive control ensures bandwidth consumption does not get out of control, prevents new kinds of traffic from overwhelming the network and allows network administrators to forecast network development. Even though such poly-chronicity is just beginning, it marks a dramatic change in the nature of the Internet.

The Internet, however, does not have one trajectory, but competing trajectories that Deleuze and Guattari refer to as *lines*. Lines appear at the start of Deleuze and Guattari's book *A Thousand Plateaus* as a means to explain their book as a complex assemblage. They write, "the two of us wrote *Anti-Oedipus* together. Since each of us was several, there was already quite a crowd. Here we have made use of everything that came within range, what was closest as well as farthest away" (1987, p. 3). Everything imaginable seems to have crowded its way into

the pages of the book hence their usage of the concept of assemblage. They offer the line as a concept to grab hold of the many threads of the book-assemblage:

> in a book, as in all things, there are lines of articulation or segmentarity, strata and territories; but also lines of flights, movements or deterritorialization and destratification. Comparative rates of flow on these lines produce phenomena of relative slowness and viscosity or, on the contrary, of acceleration and rupture. All this, lines and measurable speeds, constitutes an assemblage. (1987, pp. 3–4)

Lines bind together the leaves of a book and their characteristics – their flights, flows, segments, viscosities and speeds – all form a vocabulary to discuss the constitution of an assemblage. Both the machine assemblage and assemblage of enunciation territorialize or deterritorialize the assemblage by producing lines. Lines often disrupt the repetitions of the temporalities of the Internet. Poly-chronicity creates lines that reduce and manage Internet transmission as will be discussed in Chapter Three. The Pirate Bay, conversely, creates lines of flight to destabilize poly-chronicity as explored in Chapter Four.

This theoretical framework explains how the operation and systematic function of transmissive control that will be used throughout the dissertation. Transmission is a form of expression as defined by Deleuze and Guattari. Expression involves a becoming in the world of a message rather than its actual content. This becoming is a matter of time. The theoretical approach to time draws on the work of Deleuze, Bergson and Simondon that can be extrapolated to correspond to a philosophy of time corresponding to the many times of the Internet. Multiple becomings share time as part of assemblages. The concept of assemblage refers to bricolage of humans and non-humans with a common temporality. Deleuze and Guattari offer four key terms to understand an assemblage: the machinic assemblage, the collective assemblage of enunciation, territorialization and deterritorialization. From the millions of

packet transmissions, transmissive control functions as a collective assemblage of enunciation that expresses temporalities by producing and assigning rates of transmission. The temporality expressed has a value that is understood as a temporal economy. The Internet is significant because of its asynchronous temporal economy. This asynchronicity is under pressure from advanced traffic management software that attempts to control the transmissions of the Internet in order to create a poly-chronicity. Just as traffic management algorithms attempt to stabilize a poly-chronous Internet, pirates and hackers destabilize their efforts. The concept of lines will aid in the ensuing discussion of transmissive control and its limits. In summary, Deleuze and Guattari's concepts of expression, time and the assemblage offer the key theoretical components of the dissertation. These components will be explored using the following methodology.

Methodology

This dissertation employs a combination of experiments in software studies to augment its theoretical framework. The emerging field of software studies (Fuller, 2008b) attempts to explain the political and social ramifications of computer code such as algorithms and software. 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, p. 5). 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; Gillespie, 2010; Mackenzie, 2006; Rogers, 2009b; van Dijck, 2009) and desktop software to connect online (Elmer, 2002; Ripeanu, Mowbray, Andrade, & Lima, 2006). Inquiries into Internet routing software remain largely absent in the

literature, so this dissertation contributes a software study of the Internet. This approach draws on software studies, but it also develops new digital methods to understand how Internet routing enacts transmissive control. This overarching perspective focuses on how software processes packets along with three case studies that use specific methods to study its operation, elusion and representation.

What are methods to study software? If software "is the set of instructions that direct a computer to do a specific task" (Ceruzzi, 1998, p. 80), then what are these instructions? Even though a field of software studies has arisen, methods for the social sciences to study software remain ill defined. Other than arguing for the need to understand software – almost in a literary way – there remains few guides. This dissertation focuses on algorithms as the key lens to study software. They "do things and their syntax embodies a command structure to enable this to happen" (Goffey, 2008, p. 17). Most often, they do things either in response to human input or independent of human interaction. Algorithms in communication systems encode, transmit and decode messages. This dissertation offers three different approaches to the algorithms of Internet routing: cataloging or indexing, experimental observation and participatory research.

The first study catalogs the various kinds of algorithms associated with transmissive control. The Internet enlists all types of algorithms to route packets. Chapter Three relies on technical manuals and introductory guides to understand the algorithms enabling Internet routing. These texts offer descriptions of the different logics embedded in algorithms. Two kinds of algorithms enable Internet routing: End-to-End and Quality of Service. The study focuses on how these two sets of algorithms interpret and process packets. Drawing on the work of Beniger and Deleuze, Chapter Three will investigate the capacities of these two kinds of algorithms and how they express temporalities of the Internet.

The power of transmissive control can also be understood at its limits – the moments where it lacks dominion. The second study in Chapter Four focuses on the actual operation of different algorithms that either facilitate piracy or its capture. Evidence for this study comes from a description of peer-to-peer BitTorrent protocol as well as observations of BitTorrent traffic as observed by a commercial traffic management device called the Packeteer PacketShaper 8500 and The Pirate Bay's iPredator Virtual Private Network Service. The study watches the machine as it works and also looks at how its user manual explain how it works. A series of tests with the PacketShaper explore how it identifies BitTorrent and how the iPredator eludes its gaze. Chapter Four investigates how the iPredator service operates in order to explain how it eludes computer profiling: how it obfuscates can be seen and how it trigger traffic shaping software by ISPs.

The final study in Chapter Five focuses on transmissive control as it operates on the Internet. Studying the operation of the Internet has been a challenge in Computer Science that has resulted in the development of a number of different Internet measurement tools. These pieces of software record the operations of Internet routing to measure the network capacity of congestion (Murray & claffy, 2001; Paxson, 2004). More recently Internet measurement tools have been developed for the public to study their own home connection. These *public research tools* also expose the operations of transmissive control. Chapter Five reviews how these tools work and make recommendations on how to publicly monitor transmissive control in Canada.

All these approaches combined offer ways to study transmissive control. Though not a central task, this dissertation contributes new approaches to the field of software studies. Cataloging, experiments and public research all remain productive lines of research. Com-

bined in the dissertation, they provide offers a thick description (Geertz, 1973) of Internet routing and transmissive control.

Organization of Dissertation

Following this introduction, the second chapter investigates the inception of the Internet as a means to study its *asynchronicity*. Packet switching, a method of digital networking, allows for different conditions of transmission to occur on the same medium. The chapter offers a history of the different communication systems to distinguish the Internet from its predecessors. Communications systems have conditions of transmission and control that produce a *temporal economy*. Since the Internet can support multiple temporalities, it has successfully remediated many of these prior forms of communication. These communications conflict on the Internet making the case for more systematic approaches to its transmissive control.

The film *Inception* offers a metaphor to represent the multiple times of the Internet. The movie offers both a way to imagine the asynchronous temporality of the Internet and a way to explore the development of the Internet. The film itself takes place over four nested dreams that each take place at different rates. Time slows the deeper into the sequence a dream exists. *Inception* helps give some structure to the complexity of the asynchronicity of the Internet by giving the reader an image of multiple dreams to focus upon. Not only does the film function as a metaphor for asynchronicity, it also offers a narrative to explain the inception of the Internet. Dreams in the film drive the narrative toward its eventual climax and this structure explains all the dreams at work during the inception of the Internet in the early 1990s.

Chapter Three explores the operation of transmissive control software harnessing the Internet's asynchronicity. While Deep Packet Inspection has attracted the most attention, the technology is only part of a larger suite of algorithms enacting transmissive control (Finnie,

2009). New networking software contain sophisticated algorithms for Deep Packet Inspection, deep flow inspection and policy management. These algorithms extend the perspective and program of network management to create tiers of information delivery; creating specific durations for kinds of Internet communication (Graham, 2005). These technologies have been quietly installed into defence networks and commercial ISPs with the promise to prevent congestion and to ensure quality of service. New algorithms, specifically Quality of Service algorithms, enhance the capacities of transmissive control so that it can better manage the asynchronicity of the Internet to create a poly-chronicity of limited and optimized temporalities.

Through Chapter Three, algorithms are likened to demons as a way to emphasize their otherness to human activity. The operation of transmissive control is a story of a medium possessed by these demons. Supernatural hoofs, claws and fangs latch into messages; they travese them across vast media. Demons function as a metaphor to explain the agency and power of software during the transmission of information on the Internet. What is a demon? Dante in his journey through Heaven and Hell in the *Divine Comedy* encounters his first demon, Charon, who ferries souls across the river Styx into Hell. Dante writes, "Charon the demon, with eyes of glowing coal, beckoning them collects them all; smites with his oar whoever lingers" (1851, p. 41). Charon hints to the conceptual power of the demon, as a mythical spirit whose presence explains how something works and repeats ad infinitum. Charon is the means of passage of souls from the living to the dead, an eternal repetition. The continuous, eternal repetitions – that Dante ascribed to Charon – mimic the nature of Internet algorithms that appear demonic in their relentless information processing.

To the threat of poly-chronicity, Internet hackers, pirates and other recursive publics have recklessly flaunted authority. An anonymous manifesto circulated by the Swedish anti-copyright group The Pirate Bay, declares

> The machine, which operates under the radar frequency is unhindered.... It leaves no one unmoved and mangles everything in its path. Technically superior and physically independent it's constantly transforming, mutating and reappearing in new guises and under new codenames. With a stranglehold on its opponents it's completely untouched and even more – incomprehensible. (2011, pp. 36–37)

Their description portrays themselves as a fluid, shape-shifting machine; one always ahead of their opponent's network management. Strange swarms of humans and machines come together to fight off attempts to control the unwanted aspects of open communication. They regard network management software as a threat to their ability to communicate openly and they deploy their own software to thwart better management.

Chapter Four uses the case of The Pirate Bay and their tactics to discuss the limits of transmissive control – how the group eludes the allocation of temporalities by confusing the profiling and programming of its algorithms. Specifically, the chapter will investigate the BitTorrent protocol and the iPredator Virtual Private Network. These two illustrate different tactics – or lines of flight – for The Pirate Bay to elude transmissive control. Their iPredator is part of a larger campaign to push the limits of transmissive control. Their struggles constantly change directions, tactics and channels to stay ahead of the routines of traffic management. The Pirate Bay deliberately modulates its communication to interfere with transmissive control. Control responds by again modulating its profiling and program to capture these new modalities generated by The Pirate Bay, but how quickly can it adapt? The lag leaves a time for elusion. The case of The Pirate Bay illustrates the cat and mouse game between transmissive

control and its elusion, but it does not fully address its political ramifications. A solid discussion of their technologies maps the virtualities of transmissive control and its potential for elusion.

Chapter Four relies on the metaphor of *Moby-Dick*. The novel chronicles the voyage of the *Pequod* and its Captain Ahab as it hunts for the dreaded white whale Moby-Dick. Ahab is both a symbol of control and the limits of control. His mad quest to kill the whale resembles the struggle of transmissive control to capture elusive pirate networks. The metaphor captures how the interplay between control and its limits draws the Internet onward just as Moby-Dick's flight from Ahab drives the novel onward. Ahab, as a metaphor for control, gives some character to the largely software processes managing peer-to-peer transmissions.

The final chapter shifts to matters of policy, in part as a way to avoid the eternal hunt in Chapter Four. The chapter offers justification for enlisting citizens in studying the instantaneous effects of transmissive control. Finding a political time involves a translation of transmissive control from its instant operation into a memory capable of representing its effects to the public. This final chapter investigates projects, especially software projects, that represent transmissive control to the public. How can the processes of network software be publicly represented and perhaps governed? Media reform movements have made some steps to this end. Much of the controversy surrounding traffic management, in fact, results from public research projects. Comcast's interference with BitTorrent traffic came to light only after hackers analyzed their packets and discovered the invisible hands – of software routers and markets – interfering with their traffic. The social sciences have a vital role to play in the theorization and popularization of methods to represent the opaque technical workings of transmissive control. These public research projects develop instruments to represent packet shaping and traffic management to the public to allow decisions about its relation to the common

good. The approach implies a firm belief in the democratic experiment – the need to compose a common world together (Callon, Lascoumes and Barthe, 2009).

A final film metaphor offers a way to imagine the journey to expose the operations of software. The film *Stalker* tells the story of a journey of three travellers deep into a place full of anomalies of time and space known as the Zone. Though never *seen* on screen, the Zone is full of anomalies of time and space. The spotted landscape resembles the temporalities of the Internet where different applications might fall under traffic management policies that define its transmission. Since these moments of classification and transmission occur deep within the circuits and fibre of network architecture, they are as oblique as the hidden anomalies of the Zone. The characters in the film cope with these oblique anomalies through improvised methods and patience. Their pace and tone give the chapter a way to understand its own confrontation with oblique algorithmic process that must also be exposed.

This dissertation, in summary, elaborates a theoretical framework for transmissive control. Opening the black box of the Internet reveals the algorithms behind its routing. These algorithms enact its transmissive control. Yet, it has a finite capacity to adapt to its inputs. The Pirate Bay demonstrates how political actions entail the modulation of communication to interfere with transmissive control. However resistance from The Pirate Bay lacks the mechanisms to address the control democratically. The final case, then, involves how to bring transmissive control into the public light. These components together explain a theory of transmissive control.

Chapter Two: Inception Point

Introduction: Inception

Strangers doze mid-flight as a van crashes into a river as an elevator tumbles down its shaft as a winter fortress explodes as an imagined city dissolves. All these moments happen simultaneously during the climax of the film *Inception* directed Christopher Nolan. The film imagines a future of corporate espionage where competitors invade each others' dreams to steal or, in the case of the film, plant ideas. To plant an idea requires a complex fraud to trick the dreamer into believing the idea. Spies orchestrate a series of nested dreams to delve deeper and deeper into the mind of the dreamer toward an *inception point* where they can plant their idea. *Inception* is a film with an *asynchronous* temporality that explains the temporalities of the Internet. The narrative of *Inception* cuts between four dreams that happen simultaneously, but at different rates. Time slows as dreamers move closer to the inception point. If the audience were to watch the film *as it happens*, so to speak, they would be required to watch separate screens projecting at different rates. One dream moving faster, the other dream moving slower. If most films have a syn-chronous time, then *Inception* has an a-syn-chronous time because its nested dreams have different rates.

The film offers a popular reference to help imagine the multiple times of the Internet. Where the film occurs simultaneously across these nested dreams, the Internet stitches multiple times together as it stitches together multiple media. The Internet is also asynchronous as an assemblage of different times, vestiges of the networks it connected. This temporality requires a much more complex means of transmissive control than cinematic editing used by the film to support the multiple times.The chapter uses the film's structure of connected

dreams to unpack a crucial moments in the inception of the Internet. The film gives some urgency and pace to a long history of computer networks that can only briefly be explored in this chapter. For the dreams of *Inception* were devised and nested deliberately. Each dream has a value to the heist. The same is true for the dreams of the Internet as the different times have a rational or value system that supports them. The chapter cuts between a few different dreams of communication systems that each have their own value. Each dream then elaborates on the concept of the *temporal economy* to discuss how its synchronization, for example, created value. Even though these dreams converge into a common network, the conflict between different temporal economies causes issues like Network Neutrality. The climax of the chapter delves further into this.

A lone dreamer in both the film and the Internet organize and unite the many different dreams at work. The victim of *Inception* is an heir to a corporate empire who dreams of stepping out of his father's shadow. The dreamer of this chapter has a similar desire. Al Gore Jr. dreamed of an *Information Superhighway* like his father dreamed of motor highways. Whereas Al Gore Senior left behind a legacy of the Interstate Highway system, Al Gore Jr. hoped to leave a similar legacy for the Information Age by building a national computer networking infrastructure. Al Gore Jr., just as the heir of the film, comes to realize a dream very different from his own. A number of different dreams occupied Gore's mind as he imagined an Information Superhighway. His legislative work caused these dreams to collapse together into one common network just as they might have already been connected in his mind. While Al Gore Jr. dreamed of an Information Superhighway, he actually set in motion the dreams of the Advanced Research Projects Agency, particularly its visionary J.C.R. Licklider who dreamed of a global computer network.

A series of dreams link the vision of Al Gore with the eventual inception of the Internet. It involves a historic shift from creating *synchronous communication* to *asynchronous communication*. Synchronous communications includes foundational communication media from the information age (the telegraph and the analog computer) and the first mass temporal economies (the television and the telephone). Early computing tried to synchronize humans and computers in different ways including real-time, always-on and time-sharing networks. These attempts happened in most sectors of society not only in Computer Science departments but also by amateur or *homebrew* communities. Research in computer networks led to the development of packet switching communication – a development of asynchronous communication. Packet switching would eventually link the various computer networks into one network, an Internet. The last section of the chapter discusses this advent of packet switching technology as the inception point of the Internet. This final explanation of the Internet offers a better sense of the current tensions as well as the value of transmissive control.

Moving from Gore to Licklider to the eventual inception of the Internet through packet switching must begin with the first dream of the underlying all this chapter: the value of transmissive control itself. Behind Al Gore's initial claims was a belief new forms of communication would cooperate with economies and create different forms of wealth. He believed in the tremendous value of computer networks and its temporal economies. His dream of the value of communications and their forms of transmissive control begins this long sequences of dreams that created the Internet.

Technology, Control and Time

Al Gore Jr. was a perpetual champion of computing and digital networks as valuable communication systems. His efforts culminated in High Performance Computing and Communica-

tion Act of 1991. As the pen of then President George H.W. Bush swept across the page of the bill on 9 December 1991, it not only ratified the bill as law, but ushered in a new age of computer networks that have become the de facto communication media of the current age. Known as the Gore Bill, it turned his vision of an Information Superhighway into a reality by investing billions into the computer-networking sector. The following year, Gore would use the bill as part of election platform for a National Information Infrastructure (Lyman, 2004, p. 203). Robert Kahn and Vinton Cerf of ARPA (2000) both declared the Gore Bill to be the catalyst that put in motion the interconnections that led to the Internet.

Al Gore dreamed of the value of communication systems and their form of transmissive control to the economy of the United States. When Al Gore introduced the High Performance Computing and Communication Act of 1991, he concluded by telling congress that "the nation which most completely assimilates high-performance computing into its economy will very likely emerge as the dominant intellectual, economic and technological force in the next century" (1989, p. 276). Why would a "nation which most completely assimilates" computing "domina[te]" the next century? Behind Gore's claim is a belief that communications create valued temporalities. Though Gore never really considered time in his metaphor of the Information Superhighway, his vision recognized a value in managing an economy with communication technologies. His dream was a common one. Communication technologies have been seen as valuable because of how they express temporalities. The drive to value and economize time through a system of transmission will be referred to as a *temporal economy*. Temporal economies offer an analytic to explain the patterns in an assemblage expressing time as intelligible, regulatable and valuable. Economy is a deliberate word choice invoking both systems of exchange and comparative value between durations within a temporality, but also a sense how one temporality might be *more valuable* than another.

Transmissive control creates value by bringing together components (a function of the machinic assemblage of machines, computers, medium and jobs) with certain forms of control (a function of the collective assemblage of enunciation). A communication system might be more valuable temporal economy if its temporality enlists more components with more precision that its competitor. Certainly, communication systems have always competed with each other for capital and users – a competition that often hinges on whether the temporal economy is superior to others. Cultural historian Paul Edwards (1997) comes closest to explaining the value of communication and time when he discusses the SAGE network built by the United States Air Force (which will be discussed in depth later in the chapter). It embodied a myth of real-time strategic defence from air attacks. The network linked together radar towers with control bunkers seeking to operationalize the command and control model of military thought. SAGE, however, was the product of the Cold War so its real time control was not just seen to be more efficient, but *comparatively more efficient* than the defence systems of the USSR (Gerovitch, 2008). A better command and control model would allow the United States to react quicker and more precisely than the USSR command and control regime. Through this chapter, temporal economies will be discussed according to how their forms of transmissive control bring together and coordinate their components.

Temporalities involve a manifold of durations bound together in a past, present and future; yet, this manifold is not homogenous, but rather a heterogeneous system of relations akin to an economic system of interrelated values (cf. Callon, Méadel, & Rabeharisoa, 2002). The concept of network relations offer an insight into the economics of temporalities. If Latham (2005) offers network relations as a way to question the rationalities of connection, then the temporal economy questions the values at work in the coordination and control of different durations. Similar to how network relations sought to expose calculations of the

value for interconnection, the temporal economy seeks to question how and why components might be put into communication.

Temporal economies include senses of time in addition to the actual expression. The clock, for example, offered a different logic of calculation to understand the labour as shown by E.P. Thompson (1967) who argued that the clock shifted labour from task to time management. Hours worked allow managers to re-imagine their factories (not unlike how Beniger describes the control revolution) by rendering the past, present and future as discrete units of labour hours. Barry and Slater (2002) in their discussion of the work of Michel Callon (1998) write that economics functions with embedded forms of calculation. As they write, "metrological practices (such as those associated with for example quality control, audit or environmental monitoring, etc.) do not just reflect reality as it is. They create new realities (calculable objects) that can, in turn be the object of economic calculation" (Barry & Slater, 2002, p. 181). Certainly, temporal economies offer means of calculation in their opportunities to synchronize and distribute times. Time can be saved, conserved or intensified. Yet, these senses also involve becomings or trans-individuations of organizations that bind labourers around a whistle indicating the end of the day or even time zones that allow a corporation to synchronize their operations across the globe. The term, then, needs to be seen as both this sense of a temporality and its expression.

The rest of this chapter develops the concept of temporal economies of communication systems as a way to consider the particular conditions for the rise of transmissive control on the Internet. Many technologies – the telephone, the television and computer networks – will be introduced to develop the analytic of temporal economies. Without a sense of the value of communication systems, the impetus for creating and joining networks would be lost. The

next section discusses some of the drives to create new temporalities resulting from changes in transmission due to computing and the telegraph.

The Control Revolution

Al Gore, keeping with the theme of this chapter, dreamed that computer networks were vital to the economy. He continued his speech mentioned above by saying: "Unless we learn from them and act in time to nurture our own resources, the information age will be theirs, not ours, to lead. American technological supremacy, which we had thought of as a kind of national attribute, will pass. And so will its rewards" (1989, p. 276). Gore's belief in the value of communication in the Information Age rests on another dream that dates back to the proliferation of technologies and temporal economies in the late 1800s. Beniger argues that certain crises in industrial and social management required new technologies of time management. Industrial and politic crises, in short, required greater control over time. Improved temporal management fit within a larger Control Revolution. Where the basis of the information society underlying the Internet has often been cited as a recent development, Beniger argues "the basic societal transformation from Industrial to Information Society had been essentially completed by the later 1930s" (Beniger, 1986, p. 293).

Beniger describes the Control Revolution as a result of advances "in information-processing and communication technology" (Beniger, 1986, p. 292). Two technologies, the telegraph and mechanical computing, run throughout Beniger's history of these advances. The two represent the underlying dreams behind the modern belief in the value of communication. In exploring the two technologies, the nuances of temporal economies appear. The success of telegraphy and computing endure throughout the modern era and support Gore in his own dream of an Information Superhighway.

Electrical Telegraphy: Binding Durations Together

Electrical telegraphy marked a major industrial change due to its new affordances of transmission. Telegraphy, Carey rightly points out, distinguished the space-time of coded communication from that of transportation. Gradually, communication systems had sought to transmit coded messages faster than they could be transported. Earlier forms of telegraphy functioned through line-of-sight optical codes. Proximity allowed two parties to relay a message over a given space usually through flags or other visual signs. Most towns had a telegraph hill or beacon hill with a sufficient vista to see optical messages from afar – two by night, three by sea (Carey, 1989, pp. 162–171). Now wires conducted electrical signal faster than even a stable chain of beacon hills. The electrification of telegraphy had a similar effect as the steam engine. Both technologies separated transmission from its organic media such as the eye and the leg (Mattelart, 1996, pp. 48–49). Now communication systems could control and coordination across much greater territories.

Telegraphy decreased the time delay in sending messages and facilitated greater regional coordination, cooperation and control; in effect, the temporal economies *could be synchronized over larger regions*. One of the first uses of the telegraph was to signal trains (Mattelart, 1996, p. 51). Since information now moved faster than trains, the telegraph could dispatch instructions to operators in far away cities before a train left or arrived (Carey, 1989, pp. 165-166). Greater control allow more efficient use of the rails and avoided deadly crashes (Carey, 1989, pp. 171-175). The ability to operate with a common time drove the standardization of nationalized time (Mattelart, 1996, pp. 50-53) and eventually global time zones though it was not until 1884 that the world reached an agreement and not until 1911 before major world powers like France abided by this agreement (Mattelart, 1996, pp. 163-165). Commodity traders also felt the impact of news over the wire to alter their daily activity. They could receive the prices of goods in any

city before they shipped. Price disparities between cities lessened. Sometimes too much, as telegraph messages from the New York Stock exchange had to be delayed initially by 30 seconds to ensure the value of trading in the city (Carey, 1989, p. 169). Synchronization consolidates the forms of temporal economies. National and global markets subsume local ones. The telegraph, in other words, led to the expansion of capitalism, as the market became a general force, rather than a local one.

Changes in commodity trading also illustrate that changes in temporal economies alters the expression of past and future. Futures markets emerged after the advent of the telegraph. Commodity markets shifted from profits based on arbitrage – buying low in one place and selling high elsewhere – to futures markets, where profits resulted over time. As Carey writes, "it was not, then, mere historic accident that the Chicago Commodity Exchange, to this day the principal American futures market, opened in 1848, the same year the telegraph reached that city"(Carey, 1989, p. 168). Commodity traders shifted from profiting by knowing *where* to buy and sell to *when* to buy and sell. When Carey distinguishes between pre-telegraphy arbitrage markets and post-telegraphy futures markets, this shift involves temporal economies. Telegraphy expressed a valuable time that usurped the older economy of unsynchronized regions.

Telegraphy also altered the senses of the past. Newspapers shifted from partisan journals to journals of timely, professionalized and objective information (Carey, 1989, p. 162; Mattelart, 2000, pp. 23-25). The telegraph "allowed news – indeed, forced news – to be treated like a commodity: something that could be transported, measured, reduced and timed" (Carey, 1989, p. 163). News agencies, such as Reuters, Havas and Wolff, emerged to sell breaking information to newspapers (Mattelart, 2000, pp. 23–25; Starr, 2004, p. 180). On the leaves of an open paper the reader would find current affairs from across the nation. The rate of transmis-

sion influenced the contents of the newspaper. Since a newspaper could be delivered in less time, it could focus more on current events than punditry. Publisher William Randolph Hearst famously quipped to a reporter stationed in Cuba during the US-Spanish war, "provide pictures, I'll provide the war" (Mattelart, 2000, p. 25). Hearst clearly understood the rising value of a newspaper mediating a war as-it-happened to the public. The telegraph wire allowed daily events on the warfront to be wired back to the Hearst papers to be published the next day for reading publics now excited to read events of yesterday.

Telegraphy illustrates how the bifurcation of transportation and transmission allowed for an expansion of the machinic assemblage across greater regions of space. These components depended on a system of transmission to keep them synchronized. Less delay due to distance reoriented the value of communication systems and allowed for increased centralized control. Synchronization, however, distributed unevenly. Control concentrated in cities and in corporations. Although these tendencies are evident in the business success of telegraphy, the advent of information processing by computers offer a clearer example of how temporalities also create value by optimizing the components of an assemblage. The example of computing highlights relations within a temporal economy

Punch Cards and Computing: Leveraging Economies of Durations

The industrial revolution required a stream of wage labourers in and out of the factory. Paying wages required the factory to track their entry and exit. Factories delegated the record keeping to a gatekeeper who logged the hours of the labourer. However, the human gatekeeper could fall asleep or make a mistake. The Bundy Manufacturing Co. offered a product to solve human error: the Bundy Key Recorder in 1888. Their clock realized a desire to control labour time and advances in automatic time keeping. Advertising boasted the Bundy machine

could keep track of the employee to the minute and it could not be fooled like a human (Loft, 1995). The clock did a better job than its human counter part. The Bundy Clock exemplifies a delegation of labour into a machine and a machine altering the duration of that labour. Where once it involved a *sleepy watchman* (or so Bundy claimed), it now involved a precise machine.

The Bundy Clock repeats a pattern in the invention of analog computing that involves the transition of Adam Smith's specialization of labour into the mental production. The introduction of computing repeated throughout the 19th century in the case of Riche de Pony and the production of mathematical tables, Charles Babbage and the difference engine, the Banker's Clearing House and Hollerith and the US Census (Campbell-Kelly & Aspray, 2004, pp. 3–21; Mattelart, 1996, pp. 58–62, 2003, pp. 33–37). Each schematized complex tasks into simple stages. These stages led to the creation of a human computer role: a labourer whose function is chiefly information processing and simple analytics. Specialized jobs became targets for automation; however, the right machine did not exist. A challenge appeared to engineers who sought to replace living labour with a more reliable objectified labour. To do so, engineers programmed instructions into machines. The result was an analog computer capable of automatic information processing. Early computer scientist Charles Babbage, in the words of Mattelart, "extended the concept of labour to the operations of the mind" (Mattelart, 2003, p. 32). For Marx, a contemporary of Babbage, the advent of computing was a part of the class war – a mechanism of keeping the working class under control or else replacing them with machines outright (Dyer-Witheford, 1999, pp. 1–5; Schaffer, 1994).

Automating information processing was not a one-to-one exchanging people for machines, but a matter of calculating the optimal system of coordination. Automation involved a temporal economy delegating machines with some tasks while leaving other tasks

in human hands (similar to how Simon stresses that an attention economy must find machines that listened more than they speak). Though the history of automation is much more complicated than can be addressed here (see Noble, 1984), it involves a mathematics seeking optimal productivity – creating the most productive temporality. Early analog computing, in effect, multiplied the types of becomings, be they mechanical or human, operating in an assemblage – a history that Parikka discusses in his work on insects and other non-human durations (2010, pp. 57–84). These durations interlock in systems designed to create the optimal or most productive time. Bringing computers into contact with humans, however, required new forms of transmission that could allow systems of communication comprehendible to both humans and machines.

The punch card was one of the early forms of transmission that synchronized humans and computers. Factories issued time cards to workers, who were now expected to *punch in* or *punch out*. The act of punching-in refers to a central object of early computing – the time card. The cards acted as a point of exchange between humans and computers. Workers carried the cards with them and machines recorded the times of the workers and other personal information of the employee. The punch card was a means of transmitting hours worked between shifts. Punching the clock allowed factories to better manage their payrolls and extract more granular units of labour from its workers. Yet, this optimality of temporal relations excluded certain forms of cooperation as much as it intensified tracking the amount of time laboured. The Bundy clock did not measure quality or the intensity of labour and so intensified the shift identified by Thompson (1967). Its sense of time lent itself to a system of calculation focused solely on time laboured, rather than the quality or productivity of labour other than metrics such as units per hour.

While the roots of the computing revolution often reside in the Herman Hollerith and the 1890 US Census, Bundy was an important part of this success. In 1911, Bundy Manufacturing Co., then the International Time Recording Company, merged with Hollerith's firm and others to form the company that eventually became IBM (Campbell-Kelly & Aspray, 2004, p. 39). The merger of companies also demonstrates the value of automation as factories shifted production to more productive machines. Computers greatly increased productivity in the areas of mental labour. The 1880 Census, for example, required 1,495 clerks and 7 years for a population of 50,189,209. The 1890 census, with Hollerith's machines, took 2.5 years for a population of 62,622,250 and saved the Census Bureau millions (Campbell-Kelly and Aspray, 2004, pp. 15-19). The merger of statistics and time keeping in the predecessor to IBM allowed for superior management of the labour force (Beniger, 1986; Campbell-Kelly and Aspray, 2004, pp. 36-44). Computing, thus, begins inquiries into how shifting labour from humans to machine to realize greater organizational and production efficiency.

Computing and the telegraph spurred new temporal economies. The former illustrates how temporal economies coordinate a variety of durations according to logics of optimality and efficiency. The time clock, the punch card and the tabulating machine each illustrate a mutating and technological expansive trajectory of temporal economies. Machines proliferated with the promise to economize time and maximize efficiently. The telegraph, on the other hand, demonstrates the synchronization of temporalities across greater regions. Citizens in nation-states operated in the same market, transit system or news cycle with a common past, present and future. The telegraph alters the nature of time over space. These two factors remain central characteristics in the advance of the Internet, but first the concurrent dreams of Al Gore must be elaborated.

Figure 1: The Information Superhighway

During his speech before the Senate, Al Gore makes an oblique reference to other networks in operation that did not function fast enough in his opinion. He said:

> my proposed legislation recognizes that it is vital to respect the existing private networks, which, although of lower capacity than needed, can and must play a critical and ever-increasing role as the new high-volume network matures (Gore Jr., 1989, p. 276).

What were these "existing private networks" that had a "lower capacity"? Why would they have an influence on the development of a new computer network? An answer comes from an article the following year in a special issue of *Scientific American* on *Communications, Computer and Network*. Al Gore acknowledges that two industries were leading to the kind of convergence imagined by his dream of the Information Superhighway. He writes, "the telephone

companies want to transmit entertainment; the cable carries are asking to get into the communications business" (1991, p. 153). These two industries had become highly profitable communication systems with well-established temporal economies.

Their value – a second dream of technology unfolding new possibilities of profit and control – helped explain what the Information Superhighway would be. A cover from the January 1994 issue of *Popular Mechanics*, seen in Figure 1, shows both television stills and voices travelling across a series of tubes. The value of the Information Superhighway, according to the magazine and often in the work of Gore himself, was how new computer networks would revolutionize television and telephony. So the third dream occupying Gore's mind was one of the value of these two temporal economies that offered specific forms of synchronous communication. The following section explains how these communication systems created value in order to explain how these industries would take to this new revolutionary Information Superhighway.

Broadcasting and telecommunication economies gradually developed into profitable communication systems. They both sought to create temporalities with valuable synchronizations that crystallized the early synchronizations of the telegraph and computing into some of the largest modern industries. Today the telephone is the definition of a *one-to-one* telecommunication device that allows two people to talk at the same time and the television is a *one-to-many* broadcasting device where audiences pay attention to programming at the same. Neither began with such a clear view of their value. Williams (1990) stresses technology had to be appropriated to specific economies. Radio waves first carried telegraph signals and the telephone entrepreneurs tried to sell the device as something akin to a radio to listen to concerts far away (Marvin, 1988). Over time, the trajectory of the assemblages stabilized by leveraging the particular forms of control afforded to them by technologies and developed business mod-

els to capitalize on their abilities. The crystallization of broadcasting and telecommunication into temporal economies exerted tremendous influence over the manifestation of new communication systems, particularly computer networks as will be discussed.

The Instant World of Telecommunications

Alexander Graham Bell originally patented a device to improve telegraphy by allow lines to send multiple telegraphic signals. His patent did so by sending signals as "electrical undulations". This technique, he added in at the end of the submission, allowed for "transmitting vocal or other sounds telegraphically" as well (Bell, 1876, p. 4). This second capacity of transmission proved very popular. Bell's patent did not really understand the potential of voice so only later did telephony develop as a valuable communication system enabling direct personal communication.

Telephones as a mode of personal communication did not crystallize into a temporal economy until well into the 1920s (Huurdeman, 2003, pp. 176–180).Telephony had to prove itself against telegraphy. As Starr writes, "the telegraph seemed to meet the demand for instant communication and it had certain advantages, such as producing a written record, while the telephone at its debut was cumbersome, unreliable and limited in range" (Starr, 2004, p. 19). The telephone expressed its value as it eased participation in *instant communication*. The telegraphic network remained hard to use for the average person. The telephone entered the market as a simpler, personal telegraph. Few residential telegraph services existed due to their cost and complexity to operate in the home (Starr, 2004, pp. 194-195). Gradually firms realized the accessibility of telephony as key feature of its temporal economy. The telephone operators gradually honed their sales pitch to extol the benefits of telephone to synchronize distant

lives. Buying a telephone ushered in an instant world where anyone could *reach out and touch somebody* as AT&T famously advertised.

Connecting to the telephony network involved its own economy. Since telephony required users to be physically wired together, extending the network required building a physical infrastructure. Infrastructure cost of the network required the rationalization of any connection. Early telephone services concentrated development in dense urban areas and excluded costly rural areas. Growing the market became a driving market forces, albeit one constantly calculating the cost-benefit of each new connection. Density even had its limits as the more users in an urban network, the more complex and complex the local switching exchange (Starr, 2004, pp. 192-200). The cost of connecting illustrates how even connecting to the Internet involves its own economics.

Computers alleviated the complexity of the telephone network allowing for more simultaneous connections in less time. The first telephone switches in 1878 employed switch boys to connect lines, but these boys proved too impolite and women soon sat behind the switchboards (see Chun, 2005). Quickly, the operator became a job under tense pressures to automate. By the late 1920s most telephone services had offset labour costs by switching from manual switching to semi-automatic or automatic switching. Customers now *dialed* numbers to connect to another party rather than instruct an operator. Each turn of the dial programmed electromechanical switching systems that put two receivers in contact (Huurdeman, 2003, pp. 188-198,245-250). Bell Laboratories, the research lab of American Telephone and Telegraph Company (AT&T), drove developments in computing, such as the invention of the transistor, computing and information theory, in the holds of making telephone networks more intelligent and reliable (Campbell-Kelly & Aspray, 2004; Huurdeman, 2003; Kelty, 2008;

Mansell, 1993). These advances allowed the telephone network to grow to support the millions of people joining the network.

Telephony developed into a *telecommunications* temporal economy that operated through the production of instant modes of personal communication and profits through charging for this access. Picking up a telephone connected the caller into this *instant world* (cf. Rakow, 1992). The device simply worked when a user picked up the receiver. Telecommunication monopolies formed around a promise to always deliver this telephone service. This trajectory continues today as the principal players in Internet service provision have their roots in telephone service. With this lineage comes a perspective seeking to ensure a quality connection at all times to a temperamental computer network and to justify any expansion of the network with the bottom line. Although a very different technology, the television had also matured into a stable temporal economy after years of refinement.

Prime-Time Television

Television is a paradigmatic *broadcast temporal economy* in contrast to the telephone. The conditions of transmission had a tremendous influence on the broadcast temporal economy. Anyone could become part of network so long as they have a receiver and lived in range of a broadcast tower. Even range dissipated as a problem as extending the signal across the nation appeared a major task of early broadcasters (Socolow, 2007). Where the telephone could make a profit by simply adding nodes to their network, broadcasting had to find a way to make a profit while using wireless signals without a predetermined receiver. As Williams writes, "unlike all previous communications technologies, radio and television were systems primarily devised for transmission and reception as abstract processes, with little or no definition of preceding content" (1990, p. 37). The receiver – the audience – was only know as a silent mass

in range. Mass broadcasting raised concerns over the supposed *mass effects* of broadcasting media that defined pre-World War II communication theory. Direct access to media – unsocialized by the public viewing of theatres – threatened to turn public into an un-individuated mass prey to hysteria and propaganda (Peters, 1996). Radio and television responded to these threats by overlying a grid of programming to order their transmissions.

Programming allowed television to make a profit from advertising by selling access to valuable times. Each creates valuable *moments* that audiences buy and consume. In this way broadcasting deals with a deliberate scarcity of time. The techniques arose out of variations of techniques from theatre and cinema (Cantor & Cantor, 1992; R. Williams, 1990). The theatre and the cinema displayed performances and charged admission. Radio and television, on the other hand, could not block access to its signals, so instead it relied on revenue from attaching advertisements. Television, "has been, from the beginning, of a commercial type, with a built-in relationship between 'peak hour' program planning and the selling of advertising time" (R. Williams, 1990, p. 50). All early prime time programming during television was paid for by sponsors. Sponsors actually bought time from the network and hosted the show during its bought time (Cantor and Cantor, 1992, pp. 18-19). Scheduled programming allowed advertisers to buy sponsorship in advance and allow broadcaster to learn which programs generated advertisers.

Crystallizations of broadcasting temporal economy occurred as network time management became more granular. Advertisers forever wanted to know whom they were reaching. The science of demographics and audience studies emerged to conceptualize these audiences to advertisers. Advertising refers to an "institutionalized system of commercial information and persuasion" (R. Williams, 1980, p. 170). Surveys, viewership statistics and profiling offered a means to compute television audiences. Broadcasters could, in turn, use these demographics

to sell time on their networks to advertisers (Lewis, 2001, pp. 17–18). The television economy depended on a constant remembrance of viewers and their habits as a way to project a known past onto an unknown future. Smythe (1981) famously recognized the function of the network was to construct the valuable gaze of the audience into discrete blocks that could be sold to advertisers looking to target certain groups. Tiers of advertising emerged, such as prime time and soap operas (Mattelart, 1996, p. 287). The soap opera, for instance, intensified the value of daytime television by discovering the value of the *housewife* audience. It became very lucrative as a valuable audience for advertisers because this audience supposedly bought for the household (Cantor & Pingree, 1983; Hobson, 2003).

After years of refinement, the telephone and the television were the dominant temporal economies of the late-20th century. Central controls and quality of service expectations meant resulted in a large base of customers paying for service. The stability would not last long as Al Gore set these networks on a collision course with computer networks. The dreams of telecommunications or broadcast executives, however, differed from the research interests of Computer Scientists whom had developed computer networks (see Crawford, 2007; Frieden, 2002). Not only did the culture clash, but so too did the temporal economies as computer networks had vastly different agendas that commercial network providers.

Early Computer Networks

Al Gore realized that computer networks offered new forms of temporal economies. His pitch before the Senate took great pains to illustrate the possibilities of computer networks. In his speech, he stated:

> High-performance computing is the most powerful tool available to those who, in an increasing number of fields, are operating at the frontiers of imagination and intellect. (Gore Jr., 1989, p. 276)

He continued championing computers in his writings as well. Computer research, for Gore, did not entail designing new circuits, but the economic future of the nation. The possibilities could transform the American economy. His belief in computer networks had a sound foundation. Governments and the military had seen a potential use value for these applications, enough to fund years of work in the area. As much as Gore believed in the power of computer networks, his legislative work unleashed a whole other set of dreams developed by Computer Scientists that had very distinct goals from his own.

Beginning in the early 1950s, computer networks became a viable field of research and received massive federal funding (for a more comprehensive history see Aspray, 1988; Campbell-Kelly & Aspray, 2004; Ceruzzi, 1998; Randell, 1979). Researchers approached the problem of how to create communication systems that *synchronized* both humans and computers. Computer networks, in different ways, expressed a value or temporal economy of *synchronizing* humans and computers similar to the telephone or the telegraph. Three of the major initiatives of this era will be discussed to illustrate how they synchronized humans and computers. These projects include the Semi-Automated Ground Environment, distributed message block networks and time-sharing networks. S*ynchronous* computer networks eventually gives way to an *asynchronous* one with the advent of the Internet Protocols. The following section then outlines the temporalities of computer networks and the dreams of human-computer interface they supported.

Semi-Automated Ground Environment and Real-time Computer Networks

The United Stated Air Force became interested with the problem of air defence after the denotation of a Soviet nuclear bomb in 1949. Officials turned to researchers at the Massachusetts Institute of Technology (MIT) who recommended the Air Force build a new air defence system capable of intercepting attacks. Research began in 1951 at the newly formed Project Lincoln (later the Lincoln Laboratory) at MIT in collaboration with the RAND Corporation and IBM (Edwards, 1997, chap. 3; Norberg & O'Neill, 1996, pp. 69–74). They soon began to fund projects that might synchronize radar stations, military interception planes and computers into a command and control network. Millions of dollars in research and development, as well as new digital computers, resulted in the Semi-Automated Ground Air Defence (SAGE).

SAGE looms over the early history of computer as the first attempt to create a *real-time* computer network (Edwards, 1997; Jacobs, 1983; Norberg & O'Neill, 1996; Redmond & Smith, 2000; Valley Jr., 1985). Researchers soon began to approach the project of air defence as a problem of creating a system of *real-time* computer system (Campbell-Kelly & Aspray, 2004, chap. 7). The problem concerned synchronizing humans and computers that had different durations. The two operated at different rates, as later explained by J.C.R. Licklider who worked on the project, so that humans thinking in real-time "move too fast to permit using computers in conventional ways". He reflected on the problem of real time as follows:

> Imagine trying, for example, to direct a battle with the aid of a computer on such a schedule as this. You formulate your problem today. Tomorrow you spend with a programmer. Next week the computer devotes 5 minutes to assembling your program and 47 seconds to calculating the answer to your problem. You get a sheet of paper 20 feet long, full of numbers that, instead of providing a final solution, only suggest a

> tactic that should be explored by simulation. Obviously the battle would be over before the second step in its planning begun. (1960, p. 5)

Computing could not respond in time to permit its usage in military strategy; however, World War II had proven the benefits of computing. Thus, military leadership and computer scientists began to collaborate in the development of real-time computing.

Researchers at MIT positioned digital computing as the answer to the real-time problem. Digital computers, as Edwards (1997) makes clear, were not a logical next step for defence research. Electromechanical computers had been battle tested during World War II (Mindell, 2002); however, scientists and engineers sold their experimental research on digital computing to the Air Force with the promise that adaptable machines would be able to track and to intercept incoming enemy missiles in a complex battleground. Engineers argued digital computing could be re-programmed to adapt to varied inputs and situations whereas the physical encodings of a program in the gears and switches of an analog machine prevents easy adaptable. Computer scientists believed a digital computer would be able to store and run complex logical programs, achieving the dreams of Babbage (Campbell-Kelly and Aspray, 2004, pp. 59-91). Conventional thinking at the time would have used electromechanical computers to run the SAGE programs. Digital researchers became convinced that these analog machines operated with too much imprecision and too much delay for a real-time defence system. Digital computing, in contrast, offered the needed precision and instant response time. The campaign proved successful and SAGE move forward into digital computers, while foreclosing electromechanical research (Edwards, 1997, pp. 76-81). Digital computing soon eclipsed electromechanical systems as the dominant trajectory in computing.

SAGE created a system of *real-time control* housed in what the project called *detention centres*. From the project's beginning in 1954 to its end in 1984, the United States Air Force

built 23 SAGE detention centres at tremendous costs. These grey bunkers linked humans with computers and overlaid a grid on national airspace through radar and telephony. Centres communicated through AT&T telephone lines to receive radar reports and dispatch order to pilots in the air. Computers calculated the movement and velocity of projectiles in time enough to respond. A promotional film for SAGE includes an extended discussion of the *display-scope* that was one of what-would-now-be-called a computer monitor. It displayed the results of computer calculations; yet, the key distinction the film draws between the display-scope and the television or radar is memory. The SAGE network actually remembers its calculations and displays them on screen. The announcer claims "by analyzing the past, SAGE can project into the future" (SAGE - Semi Automatic Ground Environment - Part 1/2, 2007). Operators could use devices to intercept – to shoot down – enemy attacks in real time. Such analysis depended on IBM computing infrastructure. Each centre included two IBM AN/FSQ-7 computer systems that cost $30 million a piece – a redundancy in case of emergency (Edwards, 1997, pp. 101–102).

Real-time offer a clear use value to military purposes enough to justify the tremendous cost in actually building a real-time system. Computers not only filtered transmissions, but also enacted commands. SAGE centres, in effect, integrated military leadership with computer systems. SAGE "was a dream, a myth, a metaphor for total defence, a technology of closed-world discourse" (Edwards, 1997, p. 111). Computers played a crucial role in his concept of the *closed world* because they could provide the real-time analysis to create a representation of the world accurate enough to facilitate its control. The closed world describes a vision of the world made manageable. Computers and networks offered a means to represent and control an increasingly complex world. "A SAGE centre", he writes, "was an archetypal closed-world space: enclosed and insulated, containing a world represented abstractly on screen,

rendered manageable, coherent and rational through digital calculation and control" (Edwards, 1997, p. 104). The value of a real-time system lured the defence industry as it "became the pattern for at least twenty-five other major military command-control systems for the later 1950s and early 1960s" (Edwards, 1997, p. 107).

Computer network research did not stay only with an academic-military-industrial complex. SAGE also marked an important point of translation when real-time temporal economies shifted into the corporate sector. American Airlines launched one of the first massive initiatives to integrate computer networks into their business models. IBM worked with American Airlines to convert their insights from the SAGE project into a distributed airline reservation system similar to how telegraphy once coordinated railroads. The project's name, Semi-Automatic Business Research Environment or SABRE, was a direct reference to SAGE. The SABRE system was a massive project; it took 5 years, employed 200 technical professionals and cost $300 million dollars. SABRE, which went live in 1965, provided real-time data to book seats and to minimize overbooking using a network of IBM computers. The results revolutionized the air travel by synchronizing American Airlines' seat stock and reservation. A *real-time* SABRE system proved tremendously valuable with a return-of-investment of 25% from the American Airline's first investment (Campbell-Kelly, 2003, pp. 41–45; Ceruzzi, 1998, p. 250; Copeland, Mason, & Mckenney, 1995).

SAGE and SABRE exemplify the first of a three attempts to synchronize humans and computers in a communication system. Real-time largely attempted to develop computers responsive enough to the demands of human cognition. Synchronous communication not only involved response rate, but also endurance. Along with SAGE also came a problem of building a computer network with fail-safes that could survive local failures (also known as nuclear detonations).

AUTOVON and Always-On Computer Networks

Technologies since the optical telegraph had promised to create a secure reliable communication network. Telephone service, in particular, had prided itself on its reliability; however, the threat of nuclear war intensified the demands for an always-on system. The security of the telecommunications grid also became a major concern for the military (Abbate, 1999, pp. 8–17). When bombings of three AT&T microwave towers in 1961 disrupted national communications and some national defence communications, the blast reverberated through the military and stressed the need for a communications network that could withstand a larger attack such as a nuclear strike from the USSR (Barney, 2000, p. 68). The need for an *always-on* communications network intensified. A number of projects emerged, including the eventually realized AUTOVON system; however, the attack pushed along the work of Paul Baran, a communication researcher at the RAND Corporation. RAND was a major centre for Cold War research at the time (Abbate, 1999, pp. 8-17).

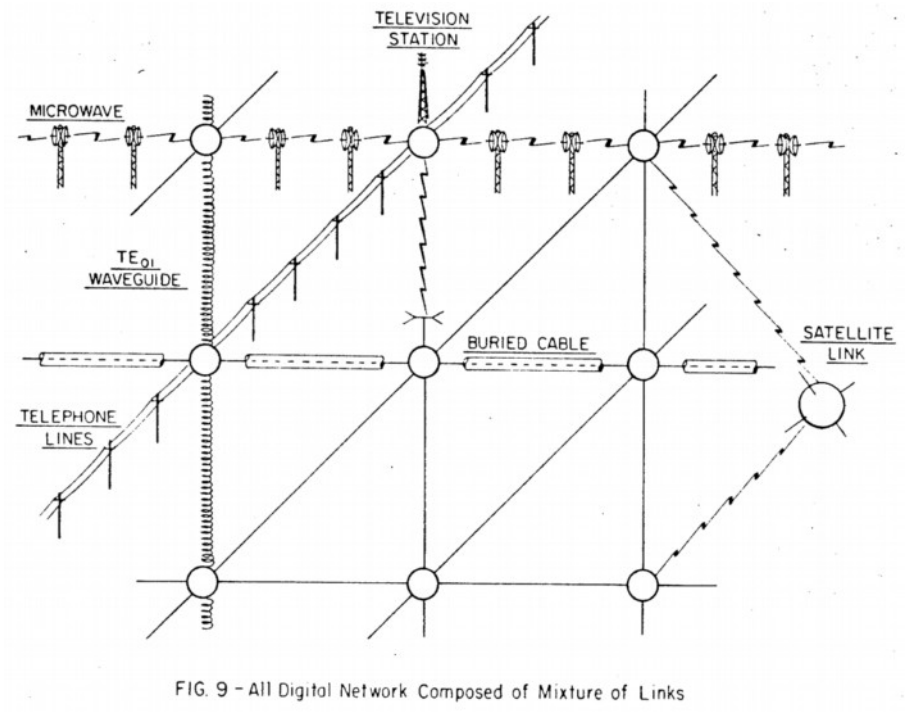


Figure 2: Illustration of a distributed network by Paul Baran

Baran (1962, 1964) developed what-he-called *distributed communications* as a way to envisage a network immune to the effects of warheads on central nodes. He sought to create networks with *survivability* – a term that measured "the ability of the surviving stations to operate together as a coherent entity after attack" (1962, p. 2). His solution involved *message blocks* coordinated by digital computers. The receiver reassembled the bits into the completed message. Figure 2 is a drawing by Paul Baran that depicts a network with a high survivability (1962, p. 24). His network is a series of distributed nodes each with a minimum of six connections. Even if a few nodes failed, a message could be successfully routed. The network could be *always on*, even if nuclear strikes crippled parts of its networks. By bringing computers into the network, Baran turned the network into a system intelligent enough to adjust routes to accommodate failures and overload (Abbate, 1999, pp. 10-20).

Baran's designed remained a proof of concept as the military had already begun using a secure network designed by AT&T known as AUTOVON. It was a *polygrid*: a network of densely linked sites that distributed traffic amongst each other. The location of each node would be secured often by being located underground. This approach differed from Baran's designs. Where AUTOVON administered control centrally, Baran required each node to possess enough *intelligence* to route and re-route traffic (Abbate, 1999, pp. 10-20). The model, in effect, embedded the computer deep with in the network. Redundant computing would allow the network to withstand and then computing around failures thereby allowing a greater chance of survivability.

Baran offered a second important temporal economy of computer networks that linked redundant computers with an intelligent network. His research would later influence researchers behind the Internet. They both saw embedding computers in the network as the key to creating robust and durable networks. In part, the switch depended on replacing

human operation switching with computers that could calculate complex routes across failures. Even though his network never attracted serious funding, he did illustrate how a network might integrate computers into its very means of transmission and, this insight along with the work of Donald Davies and Leonard Kleinrock, provided foundational for the Internet's asynchronous communication. Before this shift can be discussed, however, a final kind of computer network needs to be discussed.

CompuServe and Time-Sharing Networks

Where SAGE attempted to synchronize humans with computers and Baran depended on computers as the network itself, a third computer network sought to better share computing resources among many users. *Time-sharing* refers roughly to maximizing usage of mainframe computers by allowing multiple programmers to use a computer. Sharing the time of computer resources allowed universities to justify the expense of buying a computer (Ceruzzi, 1998, pp. 154-158). Although debate surrounds the origins of the phrase *time sharing* (J. A. N. Lee, 1992), consensus seems to fall on MIT as the nucleus of early time-sharing experiments to linking multiple people to the same computer over networks. As early as 1959, MIT had begun investigations into time sharing as a means for a computer to serve the entire university. Their usage of the term sought to create computer networks for the sharing of either computer processing or later data. MIT purchased an IBM 709 to support these experiments housed at the school's Computation Centre. Just as SAGE experimented on real-time computing, the Lab sought to create operating systems and other techniques to optimize its resource utilization between users (Norberg & O'Neill, 1996, pp. 76–98).

Time-sharing eventually became a major model of academic computer networks. The two most popular examples were USENET started in 1979 and BITNET started in 1981. Both pro-

jects emerged from the computer science departments of major research universities. USENET came from a connection between Duke University and the University of North Carolina. USENET relied on the existing tool of Unix-to-Unix Copy (UUCP) to mirror data on various computers. By keeping these computers in sync, local activities could propagate across networks to create experiences akin to communication networks. Gradually, the network stabilized into hosting mail and news groups. Newsgroups became sites of discussion for common interests. In 1984, 2,000 USENET hosts existed in the United States, Canada and Australia as seen in Figure 3 according to a projection by Brian Reid in 1986 (Dodge, 2007). Early USENET systems also connected with other networks through gateways administered in St. Louis (Quarterman & Hoskins, 1986, p. 958). USENET would later merge with the Internet to become a major online discussion forum that continues to this day.

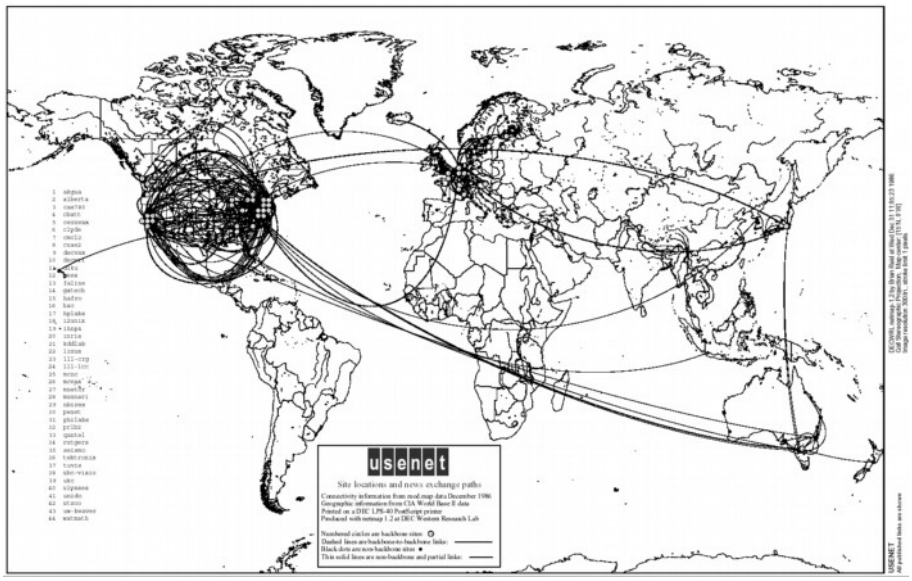


Figure 3: Map of UseNet in 1986

Another major network mirrored USENET. BitNet, Because It's Time NETwork, came from City University of New York and Yale University. It offered a similar discussion forum for programmers in the computation departments starting in 1981. In 1984, BITNET system had

1,306 hosts across the globe, including nodes in Mexico and Canada as NetNorth (Grier & Campbell, 2000; Quarterman & Hoskins, 1986, pp. 953–954; Shade, 1994). Eventually, when the networks merged into the Internet, BitNet provided the software for the first email discussion groups (Ceruzzi, 1998, pp. 298-299). These networks relied on the similar principle of time-sharing computer resources to allow for communications and shared resources.

Even though time-sharing thrived in and among universities and colleges, its real economic value emerged in the corporate sector. The commercialization of time-sharing occurred early on as MIT kept a close relationship with a nearby firm Bolt, Beranek and Newman (BBN). Computer pioneers of MIT such as J.C.R. Licklider, John McCarthy, Marvin Minsky and Ed Fredkin worked at BBN. By the early 1960s, on the advice of J.C.R. Licklider, BBN bought a Digital Equipment Corporation PDP-1. BBN sold a time sharing system to the Massachusetts General Hospital in 1963 and started a subsidiary TELCOMP that offered users in Boston and New York remote access to a digital computer (Beranek, 2000, pp. 56–60; Norberg & O'Neill, 1996, p. 86). Other firms had a similar idea as 20 other companies by 1967 had begun offering commercial time sharing services for companies (Norberg & O'Neill, 1996, pp. 104–108). These networks slowly spread from the corporate to residential sector.

One network, CompuServe, offers a clear example of the early commercial time-sharing networks. CompuServe began (as did many other firms) by selling time on computers to the insurance industry in 1969. Having computers running all the time proved inefficient. Round-the-clock utilization depended on the caffeine fuelled late nights of a Computer Science department. Come 5 o'clock, usage of CompuServe servers idled until 1978 when the firm realized it could sell off-peak time to home users at a lower cost. By 1984, CompuServe had 130,000 users in 300 cities. It sold financial analysis to its business subscribers and content as well as chat options to its home users. With the success of CompuServe came competitors, such as

the famous America Online, General Electric's Genie, The Source and the Microsoft Network. Before the Internet had begun, millions of Americans were participating in computer networks (Campbell-Kelly & Aspray, 2004, pp. 249–253; Falk, 1984).

These networks represent a third temporal economy of computing: time-sharing. Where computers had so often been designed for a single use, digital computers could adapt to a variety of tasks. Indeed, the designers of SAGE hoped computer could provide an adaptable training tool rather than a hard coded electro-mechanism machine. Where the problem began as a quest to create an adaptable computer, the challenge morphed into how best to utilize adaptable computer time. This capacity ended un creating general purpose time-sharing networks that calculated many kinds of operation at once to optimize expensive computer resources.

These three kinds of computer networks expose the various temporal economies in operation prior to the launch of the Internet. Users of any one network participated in its specific and valuable temporality. Not only did these networks offer their users different logics and economies of time, but they formed a broader economy of computing. Real-time, always-one and time-sharing networks created a spectrum of possible computer formations. Different networks formed what could be seen as a general range of possible temporalities than formed into an economy with certain relations. Real-time or always-on computing embedded computing into the logic of command, but this system was enormously expensive. Time-sharing, on the other hand, allowed users access to computing power at a much lower cost. Real-time and time-sharing could have more value at certain times and contexts. These factors certainly manifest in how organizations would later choose one kind of computing over another. These temporal economies will resurface again with the inception of the Internet.

Recursive Publics and Bulletin Board System

Computer researchers were not the only ones dreaming of computers. When Al Gore spoke of computer networks, most Americans had not heard of the SAGE or even the Internet for that matter. They likely had heard of computer networks through commercial providers like CompuServe and America Online or, just as likely, through local Bulletin Board Systems (BBSs). While researchers in the military, business and academic fields continued to work on computers, outsiders from these fields began to take interest in personal computers and networks. Hackers of all types soon began to generate their own computer networks. Advances in computer technology, cultures and infrastructures, lowered the cost of computer networks so they no longer depended on massive defence budgets. The do-it-yourself hacker ethos saw the rise of a number of computer networks patched together with existing technology and appropriated code. The emerging dream, with the nascent free software movement, believed that computer networks should be more accessible and could foster new online communities. Computer networks would be places for people with common interests to come together. These networks came to acquire great significance as visions of new forms of society – capitalist and communist alike (Barbrook & Cameron, 2001; Campbell-Kelly & Aspray, 2004, chap. 10; Ceruzzi, 1998, pp. 296–297; Kelty, 2008; F. Turner, 2006).

Bulletin Board Systems (BBS) hacked together personal computers and telephone lines to form rudimentary computer networks. With the introduction of a cheap personal modem in 1981 (Ceruzzi, 1998, p. 298), home users could connect their computers to the phone lines to establish simple networks. Users shared access to the computer as phone lines could only support one connection at a time. The ad-hoc networks became a way for citizens to start their own local discussion boards and exchanges. The Great Snow of Chicago in 16 January 1978 gave Ward Christensen and Randy Seuss enough time to create the first Computer Bulletin

Board System. By the 1990s, some 60,000 BBBs operated in the United States and thousands more likely existed internationally (Murphy, 2002; Senft, 2003; Shade, 1999).

The Whole Earth 'Lectronic Link (WELL) was perhaps the most famous BBS. It defined a key optimism of computer networks. The WELL functioned as a simple online-chat BBS in the San Francisco Bay area beginning in 1985. More than just a BBS, the WELL transitioned the counterculture ethos of the *Whole Earth Catalog* into the digital age. Turner (2006) characterized this counterculture as the New Communalist because they saw self-actualization and independence. Computers, to Brand and others, were a means of personal liberation. The network charged a modest fee in comparison to the commercial services like CompuServe. The site grew to a few thousand viewers and became a cultural icon of the Internet age. This appropriation of computing, while a marginal technical player, defined discursive formation attached to networks continues to operate on the web.

Many of the key expressions of the social value of computer networks come from the WELL. Tthe WELL and computer networks in general came to be seen by members of the site as a transformation social force finally realizing free markets. Indeed, the founders of the leading Internet rights organization the Electronic Frontier Foundation (EFF) met on the WELL. Mitch Kapor, one of the founders of EFF, states, "but when what you're moving is information, instead of physical substances, then you can play by a different set of rules. We're evolving those rules now! Hopefully you can have a much more decentralized system, and one in which there's more competition in the marketplace" (quoted in Sterling, 1992, p. 300). The WELL exemplified a new mixture of free market rhetoric and decentralized computing – an approach known as the Californian Ideology (Barbrook & Cameron, 2001). The WELL also inspired Howard Rheingold to coin the term v*irtual community*. Rheingold defined it as "social aggregations that emerge from the Net when enough people carry on

those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace" (Rheingold, 2000, p. xx). The Virtual Community that online people could overcome their difference and create a more inclusive world (F. Turner, 2006, pp. 159–162). These two values continue to rationalize the spread of the Internet.

BBSs spread across the global and formed international networks such as FIDONET. In 1983, an unemployed computer programmed named Tom Jennings began designing a cheap communication system using computers and telephone lines. Eventually, this evolved in the FIDO BBS – named after the mongrel of a machine hosting the server. Unlike home BBSs, Jennings designed FIDO hosts to share data and he released its code as free software. Anyone could use the code to create a FIDO BBS, provided it was not for commercial use. The decision to release the code mirrored Jennings own anarchist politics. By 1990, FIDONET connected 10,000 local nodes in thirty countries. The cheap network attracted activists and development workers in Latin America, Africa and Russia. Though community networks like FIDONET assimilated with the Internet, their organizations and cultures translated into creating community Internet Service Providers or new online solidarity networks (Bush, 1993; Murphy, 2002, pp. 35–36; Shade, 1999).

BBS culture included a much more subversive element than other computer network. The counterculture of Stewart Brand, the Merry Pranksters and Yippies inspired generations of phone and computer hackers who equated hacking the phone system with political dissent (F. Turner, 2006, pp. 56–68). These groups became important pioneers in the development of early computing and computer networks. Many of the early phone hackers or phreakers would start BBSs to share exploits and techniques. Often these groups freely traded stolen data and attracted the name *pirates:* a term that the music industry once applied to people make tape duplications of music (Land, 2007, p. 186). Sterling (1992) vividly describes these

hacker BBSs in the 1980s and 1990s. Hackers and pirates traded information on these BBSs or bragged about their exploits in the pages of magazines like *Phrack* or *2600*. Behind these exploits was a belief that digital systems could copy information indefinitely; thus attempts to monetize information would be futile or dangerous to the revolutionary potential of computing. Despite their sense of freedom, these BBSs were marked by secrecy and elitism as only the best pirates could operate in the top networks. Prestige and status had more currency than the value of peers sharing information freely; it would only be in later iterations of the piracy movement that hackers might try to create networks that actualized this principle (Kline, Dyer-Witheford, & Peuter, 2003, pp. 209–217; Tetzlaff, 2000).

Historian of piracy, Adrian Johns, situates its modern form within these phreakers (phone hackers) and hackers behind these many computer networks. John refers to these groups as *recursive publics* (2010, pp. 469–470). These early user-generated networks provided an imagination of what networks should be to generations of programmers. Recursive publics are "publics concerned with the ability to build, control, modify and maintain the infrastructure that allows them to come into being in the first place" (Kelty, 2008, p. 7). Hackers behind BBSs upset the establish communication order by creating their own independent networks. Hackers continue to write software to upset existing laws or orders related to digital communications (see Wu, 2003b). Behind this dissent, Kelty argues, is "an abiding moral imagination of the technical infrastructure, the Internet, that has allowed [recursive publics] to develop and maintain this affinity in the first place" (2008, p. 28). The moral imagination indicates that recursive publics share similar cultural values shaping their approach to technology. Pirates, as will be discussed, happily migrated online and soon new generations rekindled the drive to create free flows of information by developing new decentralized networks, often called peer-to-peer, to share information and files. These pirates upset the uneasy truce after the inter-

connections necessary for the Internet and prove to be a key antagonism to transmissive control.

Although these examples above represent only a fraction of the computer networks in existence prior to the Internet, they exemplify the major visions of computer networks. In a major survey of computer networks in 1986, Quarterman notes that there were over 30 different computer networks. Even with these diverse networks, three kinds of temporal economies repeat throughout early computer networking: real-time, always-on or failsafe and time-sharing. Most of these computers operated on a time-sharing logic where users managed the scarce computing resources. The Whole Earth 'Lectronic Link and piracy added to this concept of sharing by drawing in dreams of free information andv'irtual community. Although, they also illustrate the kinds of conflicts about to emerge about what forms of transmission actually realize a free flow of information or a virtual community. These conflicts would only really appear as the Internet converged and suddenly all these attempts at synchronization started to conflict.

The optimism and benefits of connection eventually drove many of these networks to connect to each other. By the 1980s, FIDONET, USENET and BITNET, along with a few BBSs had all come to connect to each other through a variety of ad-hoc gateways and protocols. A rough map of these networks, see in Figure 4 drawn by Marty Lyons (1985), charts all these interconnections.

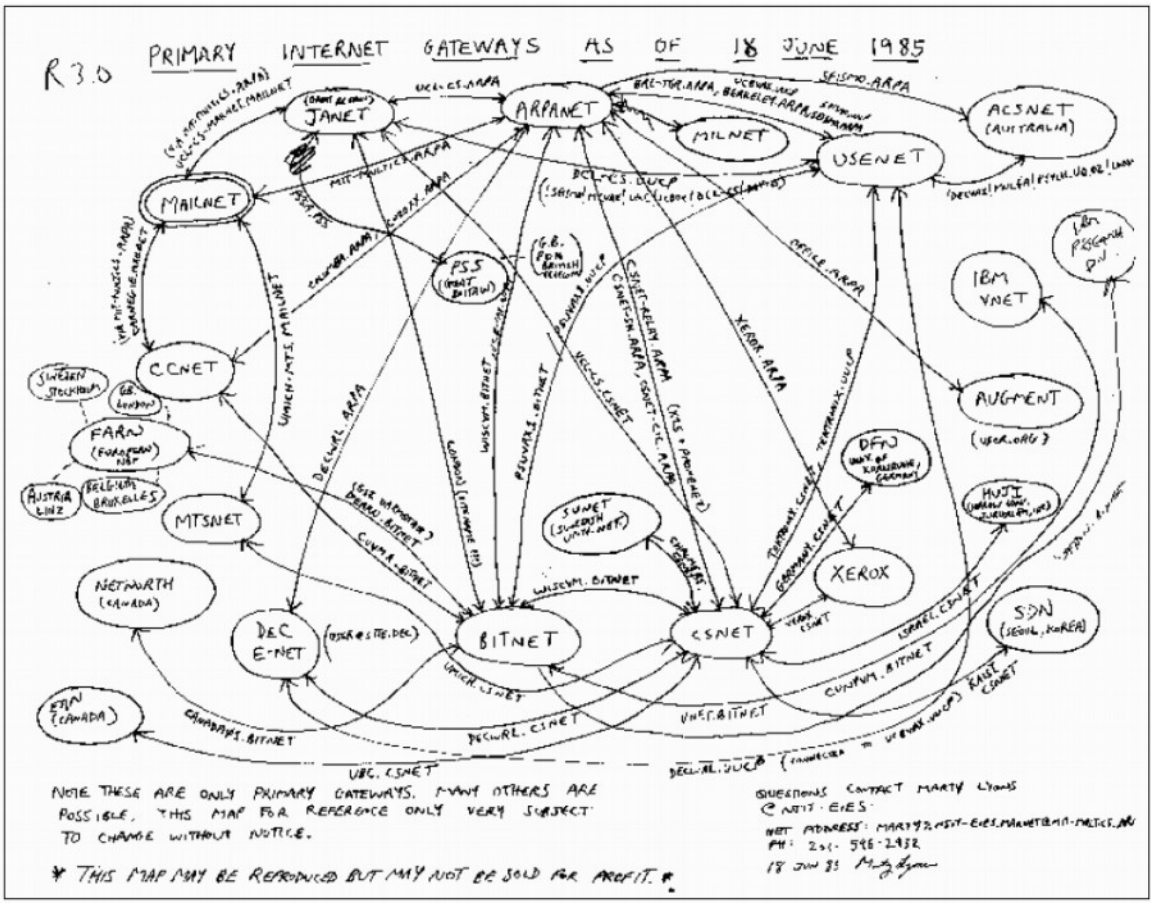


Figure 4: Primary Internet Gateways in 1985.

At the centre of the map is the one network that would enable ARPANET. Far below the dream of Gore was another dream of a global computer network. This dream, almost thirty years in the making, would be realized through the legislative work of Al Gore.

J.C.R. Licklider's Dream for ARPANET

Deep with the dreams of Gore were the dreams of J.C.R. Licklider. His vision marks the shift from synchronous to asynchronous communication. If ever there is an architect for this story, it is Licklider. Without his vision, the Internet – a network of multiple times spanning the globe – would not be possible. He rose to prominence in the United States computer research field. His own vision of a global computer network inspired both researchers and funders to

realize this dream. The following section outlines the penultimate dream of this chapter. The dream through which the inception of the Internet could take place. This dream begins with the ARPANET project in the early 1960s.

ARPANET was a project of the Advanced Research Projects Agency (ARPA) (or the Defence Advanced Research Projects Agency (DARPA) after it changed its name in 1972). ARPA emerged out of the Cold War when the United Stated had deeply invested in maintaining military superiority over the USSR. Beginning in the 1949, nuclear tests by the Soviet Union caused the United States to become more interested in air defence to protect itself from Soviet bombers. Its research agenda only led to SAGE and its interest in computer networks. Fears that America could fall behind the Soviet Union deepened with the launch of the *Sputnik* satellite on 4 October 1957. The following year, the Department of Defence launched ARPA to coordinate its research and development (Lukasik, 2011, pp. 4–6). Computers soon appeared as a solution to issues of control by its Command and Control Research project with the publication of its report appropriately titled *Computers in Command and Control* (Kita, 2003, pp. 62–63). ARPA chose an unlikely person to lead the Command and Control Research project in its new research path: J.C.R. Licklider.

J.C.R. Licklider joined ARPA in 1962 as director of the Command and Control Research project. He had varied career prior to working at ARPA since he moved from working as a psychologist on human factors during World War II, an assistant professor of Electrical Engineering at MIT where he consulted at the Lincoln Lab (Kita, 2003, p. 63; Lukasik, 2011, p. 7) and finally served as Vice-President fro the high-technology firm Bolt Beranek and Newman where he worked on digital computer networks (Beranek, 2000). While ARPA leadership saw in this experience a proven ability to lead research projects, they also had taken note

of Licklider's germinal paper *Man-Computer Symbiosis* from 1960 (Norberg & O'Neill, 1996, pp. 26–29).

This paper laid the conceptual groundwork for a research project beyond simple automation or as Licklider distinguished between "mechanically-extended man" and "man-computer symbiosis." The former refers to extending the arms and the eyes of the human with the tendency to automate human activity, where the later, as the article elaborates, aims to augment the human mind with computers. "The resulting partnership," he believed, "will think as no human brain has ever thought and process data in a way not approached by the information-handling machines we know today" (Licklider, 1960, p. 4). His insights reflected an awareness of the possible temporal economies that could leverage the comparative advantages of humans and machines; yet, his vision would not be realized until much later. After joining ARPA, his diverse background broadened the scope of ARPA's research project – a change reflected in the decision to re-name the project the Information Processing Techniques Office (IPTO) (O'Neill, 1995, pp. 76–77). Licklider re-defined ARPA's interests in Command-and-Control as seeking "improved man-computer interaction, in time-sharing and in computer networks" (1963, np.). His definition clearly deviated from ARPA's initial interests as C*omputers in Command and Control* report never mentioned time-sharing (Kita, 2003, pp. 62-63). Citing time-sharing aligned military research with computer scientist research in a formation that defined the future of the IPTO.

The vision of J.C.R Licklider loomed over IPTO and its approach to computer networking long after his tenure (Abbate, 1999, pp. 43–44; Kita, 2003; Lukasik, 2011; Norberg & O'Neill, 1996; O'Neill, 1995). Most of the original engineers and developers of ARPANET cite Licklider as a visionary who set a path for a global computer network (Kleinrock, 2010; Leiner et al., 1997; Roberts, 1978). Licklider worked at ARPA from 1962 to 1964 (Kita, 2003, p. 32). During

this time he attracted some of the best minds in computing. Researchers came from the Stanford Research Institute, University of California at Berkeley, University of California at Los Angeles (UCLA), Carnegie Institute of Technology, Information International, Inc., Thompson-Ramo-Wooldridge and Massachusetts Institute of Technology (MIT) (O'Neill, 1995, p. *77*). Prior employers of J.C.R. Licklider's Bolt Beranek and Newman (BBN) as well as MIT, particularly in the Lincoln Lab, came to have a strong influence at ARPA (Kita, 2003; Lukasik, 2011; O'Neill, 1995). As the IPTO grew, Licklider and his successors attracted a strange mix of researchers from those fascinated by nuclear war, network theory or messianic visions of a global village (Abbate, 1999; Edwards, 1997; F. Turner, 2006).

Licklider's seminal *Memorandum for Members and Affiliates of the Intergalactic Computer Network* began the conceptual steps necessary for translating his man-computer symbiosis into a computer network research. Licklider imagined computer networks as a kind of technological utopia as he described:

> Unemployment would disappear from the face of the earth forever, for consider the magnitude of the task of adapting the network's software to all the new generations of computer, coming closer and closer upon the heels of their predecessors until the entire population of the world is caught up in an infinite crescendo of on-line interactive debugging. (1963, np.)

He shared his dream of a global computer network as a *common* challenge for the both military and scientific researchers alike. In this way, Licklider was the architect for the Internet. His dream of the Internet – a common network that every computer can connect to, one that augments the minds of the world. The dream inspired generations of his successors, including the third director of the IPTO Robert Taylor (Kita, 2003). Taylor aided Licklider in elaborating on a global computer network. This vision of a global computer network, he distinguished in

a later article now collaborating with Robert Taylor, "is not new"; however, networks at the time, such as SAGE or SABRE, were only "families of machines compatible in both software and hardware and they are in the *same location*" [emphasis added] (Licklider & Taylor, 1968, p. 30). *Computer networks* in the 1960s refereed usually to time-sharing computers with multiple access terminals (Norberg & O'Neill, 1996, p. 154). Licklider and Roberts envisioned "radically new organization of hardware and software, designed to support many more simultaneous users than the current systems" – the goal being "truly effective man-computer partnership" (Licklider and Taylor, 1968, p. 31). His vision of a global computer network must be considered alongside his vision of a man-machine symbiosis. Licklider and then Taylor sought a global network of humans and machines working in cooperation; this became the technical goals of the early ARPANET.

Even though Licklider could imagine a global computer network, he lacked a technical solution to achieve his vision. He was, according to ARPA developer Leonard Kleinrock, a "visionary... not a networking technologist, so the challenge was to finally implement such ideas" (2010, p. 28). The task of achieving his dream fell upon of his eventual successor, Lawrence Roberts, the fourth director of the IPTO. Roberts found the inception point of the Internet: the concept of packet switching and *asynchronous* communication. It made possible the dreams of Licklider and Gore.

Inception Point: Asynchronous Communication

Packet switching evolved into the solution to Licklider's problem of an *Intergalactic Computer Network*. Lawrence Roberts, another former member of the Lincoln Laboratory and eventual successor to Licklider and Taylor, pulled together various threads of computer networking theory from the work of Leonard Kleinrock, Paul Baran and Donald Davies. From

1964 to 1968, Roberts developed a proposal for the future of ARPANET (Lukasik, 2011; Roberts, 1978). Where Licklider had a dream of a global network, Roberts sought to bring this dream to fruition by developing the necessary technical measures. These measures came to be known as packet switching. Lawrence Roberts first heard of the concept of *packet switching* at Association for Computing Machinery (ACM) Operating Systems Symposium in Gatlinburg, Tennessee in October 1967. He learned of the concept when talking with Roger Scantlebury who attended the conference to present his work with Donald Davies on packet-switching networks (Abbate, 1999, pp. 37–38; O'Neill, 1995, p. 78). Even though Davies's packet switching never manifested in the United Kingdom (Abbate, 1999, pp. 21–35; Campbell-Kelly, 1988), his ideas encouraged Roberts to develop packet switching as the principle behind the ARPANET. As he integrated packet switching into ARPA they also drew on the work of Paul Baran's work at the RAND Corporation on distributed message block networks as well as the work of Leonard Klienrock on computer networks. Their work eventually formalized into the protocols of the Internet (Abbate, 1999, chap. 1; O'Neill, 1995).

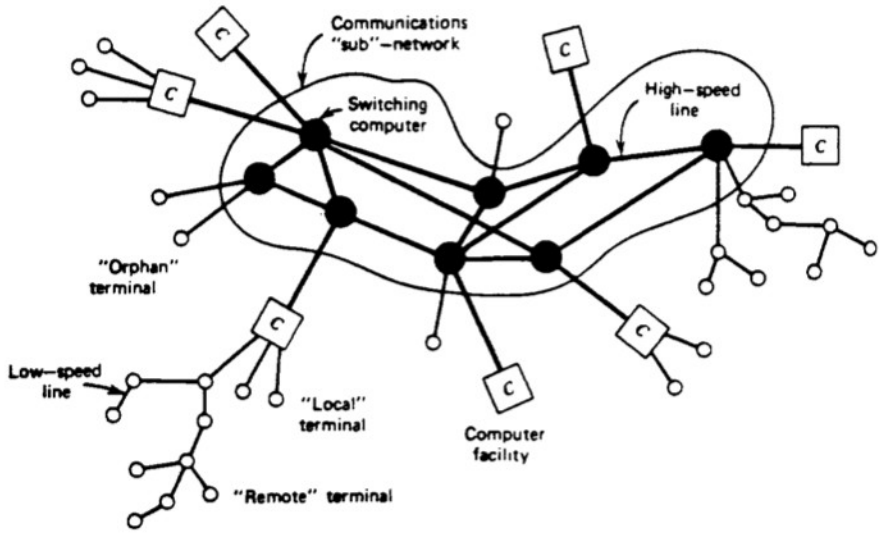


Figure 5: The structure of a computer-communications network

Packet switching functioned by breaking messages down in discrete blocks of data or *packets*. A message might contain a number of packets. Computers, what would be called Interface Message Processors (IMPs) to ARPA, calculated the encoding and decoding of packets similar to SAGE. Packets would be transmitted across leased lines from one computer centre to another. Unlike AUTOVON, however, the IMPs could independently calculate an optimal routes. Figure 5 comes from a drawing by Leonard Kleinrock explaining a packet-switching network (Kleinrock, 1978a, p. 1321). The multiple links per node resembles the network patters of Paul Baran. The "switching computer" in the "Communications sub-network" would facilitate the exchange of data between computer facilities indicated as C in the diagram. Computer switching also allowed different computer facilities, perhaps running IBM or DEC computers, to communicate with each other because it translated the different outputs into a common packet protocol (Kleinrock, 1978a). The workings of packet switching will be discussed in more depth in Chapter Three, but for now it is important to recognize how the technique differed from conventional computer networking.

Packet switching was a departure from attempts for *synchronous communication* and instead sought *asynchronous communication.* The roots of this switch were already beginning in the ideas of Licklider on man-computer symbiosis where he sought to optimize their different rates. The shift is most clear in the work of Donald Davies from the National Physics Laboratory in Teddington, United Kingdom. He devised packet switching to accommodate shared networking after realizing that data communication standards were a major impediment to popularization of computer. Davies developed a similar system of packets with Paul Baran albeit with very different intents. Telephone and telegraph networks were designed for "synchronous transmission" and "design[ed] for human use and speed" (Davies, 1966, pp. 1–2). Computers operated at different rates and could technically share a network if a system could

optimally distribute their usage. He realized that "there are two very different kinds of terminals attached to this network; human users' consoles or enquiry stations working at very slow speed and real time computers working at high speeds" (Davies, 1966, p. 5). Davies, in other words, realized that computer time-sharing, like CompuServe, managed multiple durations on one computer, so the most-efficient network would be one capable of *asynchronous* information flows. Packet switching operationalized time-sharing as computers operating at different rates could send their packets along a common network. It expanded the types of connections possible on the networking by delegating computers with the complex task of managing multiple temporalities. Computers, in other words, facilitated greater synchronization by allowing the cooperation of multiple, distinct durations.

The work of Donald Davies on packet switching created the technical conditions for a new kind of *asynchronous* communication system. Asynchronous communication could modulate its transmission of packets for various kinds of communication. An outcome of Davies' goal to create a network that could share its resources among a diverse group of users and machines. The move both adapts to the rapid multiplication of computers and links these durations together through asynchronous networking. Where prior networks had sought to streamline the types of computers attached to the network, Davies realized the diverse temporalities in computing. Asynchronization, to Davies, involved managing the multiple durations of a network to accommodate greater diversity. In doing so, he created a kind of asynchronous transmission whereby media can transmit various kinds of communication.

Asynchronous *transmission* facilitated many networks and their temporal economies into one network. The process resembles the concept of *remediation* developed by Bolter and Grusin. They write, "our culture wants both to multiply its media and to erase all traces of mediation: ideally it wants to erase its media in the very act of multiplying them" (1999, p. 5).

Asynchronous communication remediates other media, but by reducing their differences to simple different rates of sending packets, it overlooks the real differences and tensions between these different uses of networking. It should come as no surprise then that the history of the Internet is full of political and policy controversies over effective regulation as will be discussed later in this chapter. At once, the Internet collides senses of networking together and at the same time, ignores these traces of remediation.

Asynchronicity is a time capable of being any time. Both Castells (1996) and Hassen (2007) touch upon asynchronicity in their respective *timeless time* and *connected asynchronicity*. Internet transmission can offer both time-sharing and real-time. This capacity suggests a particular form of modulation. An example of another form of modulation helps distinguish the Internet. Lazzarato describes video as a modulation. A video camera modulates magnetic film to capture light and create a fixed recording. The product – the video recording – is a specific crystallized temporality. Recording, he writes, "fixes 'this modulation' on a support" (2007, p. 111). The modulation is the change in light encoded on a tape. Though a remarkable feat of recording or encoding, the video has a fairly simple means of modulation in its recording of the event in tape. The modulation synchronizes the tapes magnetic coding with changes in light and sound (2007, pp. 110–112). The Internet is a much more complex modulation of transmission in that it can capture multiple expressions at once (almost like a Lomography camera) and, more to the point, manipulate how it expresses a transmission in real-time. It could delay, accelerate and stop capture depending on its programming. Asynchronous communication, as envisioned by Donald Davies, allowed for a communication system with a more dynamic modulation, creating many crystallizations of time. Therein lies the nuance in the concept that is both a same time and a different time. Given this modulating time, various usages of the Internet have chaffed.

Packet switching as asynchronous communication proved to be the idea necessary for the creation of the Internet. The line of research allowed multiple rates of transmission at once thereby creating the technical possibilities for the remediation of the telephone and television, real-time, always-on, time-sharing and the virtual community into one singular network. Just as the idea of the film *Inception* had multiple dreams at once, packet-switching brought these systems into contact one network with multiple times. It became the technical means for an inter-networking. As Al Gore signed his bill, he set packet switching on a path to connect these prior networks into one *Internet*.

The Arrival of the Information Superhighway

While the growth of ARPANET into the Internet has been documented in detail elsewhere (for a few examples see: Abbate, 1999, 2010; Ceruzzi, 2008; Latham, 2005; Moschovitis, 1999; Murphy, 2002; Norberg & O'Neill, 1996; Salus, 1995), a few details about its success should be noted. The network expanded rapidly, in part, due to the design of the Internet protocols. The capacity to mediate multiple temporalities was an explicit design goal of TCP/IP who tried to create a protocol with low resource requirements and flexible bandwidth requirements. Router and gateways assumed information would flow with different rates and reliabilities. These technical challenges lead to the refinement of a packet-switching system that could accommodate network heterogeneity. As ARPANET standards evolved, members began to develop new applications for the network. The flexible ARPA protocols allowed users to utilize the networks for a variety of types of transmissions. By 1971, a version of email had been developed and installed on hosts around ARPANET. The file transfer protocol, on the other hand, focused on allowing users to exchange computer files. Each application adapted the ARPA protocols to send different kinds of information, at different rates. ARPA

designers adopted the openness of their protocols as a design goal – embracing user-generated content early on. Even though TCP/IP lacked formal government approval, (the State Department even endorsed its competitor OSI), it succeeded because of its ease of deployment and low requirements for network reconfiguration (Latham, 2005; Russell, 2006). These factors helped popularized ARPANET; however, one other vital component propelled its research into a heterogeneous, packet switching network.

The Gore Bill collapsed the different institutions and temporal economies into one network mostly held in the private sector. At the time, the ARPANET had been placed in the stewardship of the National Science Foundation in 1986. Gradually, the NSF began outsourcing the management of its network. Abbate writes, "NSF saw commercial operation of the Internet as a means to an end: a robust, high-speed, economically sustainable information infrastructure for scientists" (2010, p. 10). NSFNET contracted out network service to MERIT, a consortium of the State of Michigan Strategic Fund, IBM and MCI (Abbate, 2010, p. 12). IBM and MCI asked for a commercial service to recuperate their investment in the NSF backbone (Cook, 1993, p. 5). NSF agreed and in June 1990, the newly formed Advanced Network and Services (ANS) began providing the network backbone for the Internet, subcontracted by MERIT (Abbate, 2010, p. 15). The move merged commercial on ANS with the academic traffic of ARPA (Cook, 1993, p. 4). The superhighway begins with this first collision.

Beginning in 1991 with the attention Gore gave to computer networks, the NSF began getting pressure over its relationship with the commercial ANS. This pressure translated into NSFNET governance moving into the private sector (Ceruzzi, 2008, p. 29). The move put pressure on NSFNET to connect to more than ANS and also to liberalize its Acceptable Usage Policy to allow commercial traffic. NSF gradually decentralized its network contracts among four major network providers in 1994. After it had established a national data sharing

between the major commercial networks, the NSF pulled out of the network entirely, leaving the Internet backbone under commercial management. Five provider ran the Internet backbone in the United State by 1997 (Shah & Kesan, 2007, pp. 96–103). Where the NSFNET might not have been as accessible prior to the Gore and privatization, it was more decentralized. The cost of realized the dream of the Information Superhighway was the consolidation of network diversity into a single network largely under the ownership of the major telecommunications and broadcasting firms.

Even though Internet transmission could support these multiple networks, temporal economies clashed with each other. Piracy, security, over-the-top broadcasting and peer-to-peer telephony all have become flash points where tensions between the various network assemblages converge on the Internet. The Internet infrastructure struggled to support all these temporalities. Media conglomerates of both broadcasting and telecommunications temporal economies have been particularly at odds internally over how to manage these issues. Should their approach to the Internet fall within a temporal economy of broadcasting or telecommunications? Should networks police their traffic? The situation has only worsened as ISPs have faced a bandwidth crunch for on-demand movies, streaming video, multiplayer games, music stores, not to mention the explosion in illegal file sharing. The crunch, in short, requires better management of the scarce resource. But the collision of peer file sharing with telecommunication firms seems dull compared to the threats of Mike McConnell, former director of the National Security Agency in the United States. He stresses the insecurities of the Internet in his public relations campaign on behalf of traffic management software firms. He states, "we need to reengineer the Internet" because "if an enemy disrupted our financial and accounting transactions ... or created confusion about the legitimacy of those transactions – chaos would result" (np.). His security background comes with a belief that the Internet

should be *always-on* because it drives the American economy. Always-on temporal economies require the securitization of the network – bunkering down; yet, the openness of time-sharing and to a lesser extent telecommunications, have not considered the need to secure networks for users. The more redundancies in the network, the better.

The inception of the Internet has lead to many conflicts over the network itself and its dominant temporal economy, but none perhaps as fierce and as decisive as the emergence of peer-to-peer (P2P) file sharing, a new form of piracy. Successful file-sharing offered a mode of transmission that disrupted the conventional broadcasting temporal economy. At first, the associated media industries tried to sue P2P out of existence, but when that failed they moved increasingly to transmissive control to contain threats. Technology instead of law could solve the problem of file-sharing – example of a believe of what Gillespie (2007) calls a *technological fix* where social problems attempt to be solved by technology. Transmissive control is another example of a technological fix. As a way to transition to the emphasis on transmissive control in the rest of this dissertation, the following section re-introduces the problem of pirates for network administrators.

Computer Piracy and Peer to Peer

Beginning in late 1999, messages began appearing on online newsgroups discussing a new program called Napster. One user by the name of *emceeology* posted to the alt.rap group, "I am mad keen to download some mad hot tunes with the aid of the best MP3 finder on the net http://www.napster.com" (emceeology, 1999). Hundreds of messages appeared on news groups discussing Napster, its legality and their sudden ability to easily share files among each other. As Jay stated in alt.music.mp3, "[Napster] seems to be a community of users rather than a website." For Internet publics who normally had to deal with MP3 sites that "were fleeting, buried,

dilapidated and outdated" (Gillespie, 2007, p. 43). The inaccessible state of computer file sharing prompted Shawn Fanning, a Computer Science student at Northeastern University, to create Napster. Fanning recognized peers could share music files, if the technical requirements to do so lowered. Napster had two major technical innovations. First, users could easily upload, as well as, download files. Home collections created a vast resource of free, typically, music available without compensation to its producers – what some called *pirated* music. Second, Napster made searching for files easy. The program kept a database of the collected, distributed music resource on a central server that users could search. With one new application, home users could share their personal collections of music and, in return, access a vast resource of music (Gillespie, 2007, pp. 40–50).

Where once pirates and gurus had seen computer networks as a space of virtual community and sharing, now pirates realized the Internet could create a vast digital commons of copyrighted media (cf. Strangelove, 2005). Napster harnessed the Internet's asynchronicity to create a vast network of file sharing at a scale never before possible (see Gillespie, 2007; Johns, 2010). The decentralized sharing of Napster, however, directly conflicted with the temporal economies of telecommunications and broadcasting, in no small part because of their dependence on centralized control of their temporalities. Though often criticized for being slow to react, the great media firms eventually responded.

Just as the application reached critical mass, the incumbent media industries stepped in to dismantle the emerging file-sharing network. A lawsuit filed by the Recording Industry Association of America began in 1999 and ended in July 2000. The ruling drew heavily on the famous Sony v. Universal or the "Betamax Trial". The case pitted the Sony Betamax videocassette recorder against the film industry represented by the Motion Pictures Association of America. The high-stakes trial became the benchmark case in deciding the legality of a new

digital duplication technologies. The test simply asked whether a device's capacity to break copyright would overshadow its legal uses. In the Betamax trial, the judge ruled in favour of Sony because its VCR had substantive non-infringing uses. In the Napster case, the judge decided against Napster because its users were overwhelming infringing, especially since the company's central servers could filter infringing content – a capacity unavailable to Sony during the production of the VCR. Fair use did not enter the ruling as it did in the Sony ruling because Napster could control for infringing materials. The ruling did not shut down Napster; rather, it requested Napster remove infringing content from its search index and ban users sharing infringing content. The court, in effect, ruled Napster had to control communication in its peer-to-peer network in order to obey copyright laws (Gillespie, 2007, pp. 6-7; 40-50), but the tremendous cost of developing a filter and the growing alternatives to its networks effectively brought the firm crashing down.

Successors of Napster all met similar fates and most companies offering P2P software closed as a result of lawsuits from trade groups for motion picture studios and major record labels (Austin, 2005; Samuelson, 2004). These industries worried that the free flow of information would destabilize their intellectual property. Corporate lawyers leveraged regional laws to ensure that file-sharing would never be a profitable business across the globe. As Leyshon states, "the legal victories of the RIAA and its clients over the likes of MP3.com and Napster were made possible, in part, by the geography of their computer networks. Both firms operated central computer servers, located at their headquarters, which co-ordinated the networks of users that drew on their services" (2003, p. 550). As a result, regional copyright law ensnared piracy sites that collapsed after prolonged legal battles in exhaustion and ruin. Napster and its successors narrowed the window of legality for P2P networks across the globe.

Programmers of all types began to cluster around developing P2P development – attempting to develop a P2P network that could not be shut down like Napster[3]. Its failure, to many programmers, was a technical problem that could be fixed with better code – a common attitude among the recursive publics (Kelty, 2008). Hundreds of solutions emerged to varying degrees of success[4]. Some merely copied Napster, like OpenNap. Others, such as Kazaa, Morpheus and AudioGalaxy, attempted to succeed whether Napster had failed by creating a profitable company distributing file-sharing software. A few, like Gnutella and MojoNation, radically rethought how to control P2P communication to create radically new networks. Conferences sprung up for developers to meet, share technical solutions and discuss the social implications of P2P. O'Reilly, a leading computer book publisher organized the O'Reilly Peer-to-Peer Conference, February 14-16, 2001[5] which led to the publication of an edited book, *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. Many developers associated with many of the leading P2P networks, including Gnutella, FreeNet and MojoNation, contributed chapters. Most developers expressed explicit political aims in their writings. Kan, of Gnutella, states that "decentralized peer-to-peer may spell the end of copyright and censorship" (2001, p. 122) – a politics coded into the Gnutella project. In fact, most of the projects tried to create a P2P network that could not be censored. Other goals include creating a network that could not be taxed or regulated. Others still saw P2P as a more equitable mode of communication than broadcast networks. The book exemplified how the long-standing values of the *Wired* generation (Barbrook & Cameron, 2001; F. Turner, 2006). All these P2P developers sought to accelerate the decentralization growth of their networks.

---

[3] For a discussion of reactions to the Napster decision by prominent members of the P2P community, see http://archive.salon.com/tech/feature/2001/02/12/napster_reactions/print.html

[4] For a list, see: http://www.infoanarchy.org/en/The_Halls_Of_The_Dead.

[5] For an agenda of the conference, see: http://www.openP2P.com/pub/a/P2P/conference/index.html.

The efforts of P2P movements – as will be discussed in detail in Chapter Four on The Pirate Bay – meant P2P did not disappear despite countless lawsuits. Given this inability to outlaw P2P through law, copyright industries and networks turned to controlling transmission itself. Advanced traffic management software offered a solution by attempting to harness the asynchronicity of the Internet. As discussed in introduction, the digital enclosure, as a concept, falls short at explaining the reliance on transmissive control since it emphasizes the struggle has moved away from lawsuits and raids into the very heart of the network. Routers and switches now combat pirates and file-sharing as the struggle shifts from a spatial game of outrunning or being ahead of the law to a temporal game of creating windows of opportunity that momentarily elude a more ubiquitous control. The tendency as will be discussed throughout the rest of the dissertation is a movement from law and legal enclosures into a struggle over transmission itself.

Conclusion

The modern Internet continues to deal with the consequences of its own inception. The climax of *Inception* involves one stimulus or *kick* that brings all the nested dreams crashing together. For a moment, each dream effects each other. Though this lasts for only a moment in the film, the whole of the Internet is made of this moment of intersection and resonance. Asynchronous communication enabled by packet switching allows for the Internet to support multiple temporalities and temporal economies. The various economies conflict with one another. Pirates undermine the exclusivity of content and thereby the value of television programming that depends on creating valuable moments for advertisers. The plurality of time-sharing chaffs with the priorities of a real-time system. These conflicts drive the struggles over transmission on the Internet and inform the next chapters.

This chapter advances the overall dissertation by describing the context of transmissive control. At the heart of this assemblage is packet switching that functions as the collective assemblage of enunciation to produce its *asynchronicity*. This asynchronicity differs from other networks discussed in this chapter and, as a result, makes transmissive control ever more important because it can modulate or adapt to different forms of communication. With the rise of threats like piracy to network owners, there has been a drive to leverage the capacity of transmissive control to greater manage the temporalities of the Internet. The next chapters seek to expose and develop this conflict over transmission.

This chapter also develops the secondary concept of the temporal economies. Temporal economies provide an analytic to compare how forms of transmission express, quantify and represent temporalities. How does an assemblage crystallize a past and future in a present? How does it assign this temporality? Who participates – human or machine – in this economy? Economies differ in how their temporalities synchronize regions or durations and how they enrol multiple durations, such as computing. Real-time as Edwards makes clear in his discussion of the SAGE defence centres required computing fast enough to respond in time to chart movement without a significant lag (1997, pp. 100–101). The technological advances of SAGE occurred in large part because real-time control requires a certain complex of temporal relations between observation towers, computer displays and military officers. This chapter also introduces a number of economies to demonstrate the malleability of assemblage and the possible expressions of time.

The shift from legal approaches to traffic management raises some unanswered questions about the operation of transmissive control. Advanced traffic management software offers a way to capture and control the Internet's asynchronicity. The next chapter seeks to explore this operation. How does traffic management software operate? What are the algorithms at

work? In order to study the struggles on the Internet the dissertation shifts from this history to discuss the operation of transmissive control. The focus turns to the very algorithms routing packets. These algorithms enact transmissive control and the next chapter first offers a breakdown of how these algorithms synthesize time at the moment of transmission. Different algorithms have very different approaches or capacities in this moment of transmission. Chapter Three discusses the differences in the major algorithms of the Internet to illustrate how they express its asynchronicity. As will be seen, newer algorithms have a much greater control over the rate of transmission and have begun to better manage its temporalities and produce a *poly-chronous* Internet.

A new metaphor offers a way to stress the agency and the power of these algorithms in expressing the Internet. Demons – a term dating back to computer hackers at MIT in the 1960s – anthropomorphize the processes of algorithms as supernatural beasts forever toiling at routing packets. Demons have long been imagined by the likes of Dante to explain systems of control. They also inspired early computer scientists who imagined their programs as a chorus of demons working in operation. They named their program *Pandemonium* after the capital city of the demons. The next chapter suggests the Internet resembles a Pandemonium with the work of thousands of demons conflicting, but also acting collectively. This pandemonium is changing for a disorganized chaos of asynchronous communications to a new poly-chronous communications. The shift has tremendous implications for the nature of transmission online as will be discussed.

Chapter Three: Pandemonium

Hurld headlong flaming from th' Ethereal Skie

With hideous ruine and combustion down

To bottomless perdition, there to dwell

In Adamantine Chains and penal Fire,

Who durst defie th' Omnipotent to Arms.

Nine times the Space that measures Day and Night

To mortal men, he with his horrid crew

Lay vanquisht, rowling in the fiery Gulfe

–Paradise Lost, Book 1

Figure 6: Satan cast from Heaven, woodcut by Gustave Doré

Introduction

This chapter explores the operation of transmissive control through an investigation of key algorithms of Internet routing. These algorithms enable the asynchronicity of the Internet by modulating the rates of transmission to support multiple temporalities. Where the last chapter focused on describing the various temporal economies of the media before the Internet and now part of it, the following chapter seeks to explain Internet control. This chapter catalogs the various algorithms transmitting packets on the Internet. What algorithms enact transmissive control? Two major categories of algorithms appear during this cataloging: End-to-End (E2E) and Quality of Service (QoS). The former has begun to eclipse the latter to

define the assemblage of the Internet. These algorithms express a temporality system of dynamic and tiered transmission. The asynchronicity of the Internet depends on E2E algorithms, each capable of setting their own distinct times. This asynchronicity, however, is dissipating as a result of advanced traffic management software, typically QoS, that is seeking to better manage the temporalities of the Internet. Poly-chronicity prunes and tiers the temporalities of the Internet. This later poly-chronous temporality promises to define the Internet in the future.

This chapter offers a new metaphor to characterize the work of algorithms: demons and Pandemonium. While demons usually refer to supernatural beings, demons also thrive in the history of communication and control (Hookway, 1999; Roderick, 2007). Computer programmers at MIT in the early 1960s jokingly named the software running on their computers as brethren of Maxwell's demon (Raymond, 1996). Demons all the way back to Rene Descartes offer an imaginative way to describe the control of transmission within a medium. Descartes proposes the *evil demon* as a thought experiment to explain his philosophical scepticism. If "some malicious demon of the utmost power and cunning has employed all his energies to deceive me" (1996, p. 15), then Descartes could not trust his senses. An evil demon, he imagined, had the power to manipulate his perception, thwarting Descartes' quest for the truth. The thought experiment appears to have inspired physicist James Maxwell to conduct his own thought experiment with demons (Heimann, 1970, note 90). Maxwell's demon according to Beniger (1986) grounds modern engineering control theory. Demons enter his work during his writing on thermodynamic theory (see Maxwell, 1872). Maxwell imagines a demon tirelessly transmitting gas particles between two chambers to explain paradoxes of entropy. The constant, automatic and dynamic efforts of demons makes control possible. If exorcized from the system, gas particles could not pass from chamber A to B (Beniger, 1986, pp. 44–48). Again

the demon appears as a powerful being capable of observing and managing complex systems. Whereas Maxwell regards his demon as a problem to thermodynamics, Norbert Wiener sees the demon as the embodiment of information theory. Wiener seizes upon Maxwell's demon to exemplify how information processing counters entropy. Demons could be found everywhere – working to prevent entropy through their active control of a system (1948, pp. 58–59). Wiener turns Descartes on his head by using demons to perceive media, not to mediate perception. The demon offers a rich metaphor to describe the inhuman agency of software and control on the Internet.

Demons thrive on the Internet and their collective activity is also a metaphorical resource. Communications policy scholar Sandra Braman, following Hookway (1999), describes the modern communication systems as *pandemonic* – a word adapted from the name of the capital of Hell, Pandemonium, in John Milton's poem *Paradise Lost*. She writes,

> the current environment might be described as 'pandemonic'... because it is ubiquitously filled with information that makes things happen in ways that are often invisible, incomprehensible and/or beyond human control – the 'demonic' in the classic sense of nonhuman agency, and the 'pan' because this agency is everywhere. (Braman, 2003a, p. 109)

This chapter takes up her provocative claim by describing the key algorithms or demons distributed *everywhere* on the Internet. The end of this chapter seeks to describe the Pandemonium of the Internet – a capital full of E2E and QoS demons. Further, the work of QoS demons and their drive toward *poly-chroncity* involves a change in the collective assemblage of enunciation of the Internet whereby core demons in the network have more authority over network transmissions. The concept of pandemonium offers a metaphor to understand how the coordination of demons might be changing as a result of QoS.

Demons and pandemonium aid in the question to understand the nature of transmissive control. If transmissive control expresses the duration of a message, then the steady hands of demons – pushing or pulling at a message – play a central role in this duration. How then do demons possess media? How do they explain a transmissive control? How do they cooperated? This chapter seeks to name and understand the demons of the Internet. It begins by outlining a method to study the demons of the Internet based on their perspective and programming. After putting forward this analytic, this chapter catalogs the different types of software enacting transmissive control on the Internet. From this list, Quality of Service demonstrate a move to tier and manage the temporalities of the Internet into a poly-chronous temporality. The conclusion, thus, relates the questions of demons and transmissive control back to the concept of temporal economy as a way to stress the importance of this emerging *poly-chronous* temporality.

Software Demon: Algorithms of Digital Transmissive Control Software

The following section provides an analytic to understand the operation of transmissive control. This analytic builds on prior definitions of control and uses terms from these definitions to develop a more robust explanation of transmissive control. Control, according to Beniger, involves "goals toward which a process is to be influenced and the procedures for processing additional information toward that end" (1986, p. 40). Clearly two operations seem at play here: the first being an ability to read information, such as binary streams; and the second being the ability to have an effect, such as the instructions in programming. However, the definition gives Beniger a wide berth to explore control in telecommunications systems, railways and even retail stores. How does this definition manifest in forms of control online?

The definition of Beniger may be extrapolated to provide two terms to understand the operations of algorithms: perspective and logic. Perspective refers to what aspects of a packet are read by the algorithm. Network algorithms read the instructions in each layer in a particular sequence or with a particular depth. Logics refer to how algorithms respond to packets based on how it perceives information. The perspective informs the relation of the program to the packet. By exploring these two components, a vocabulary appears – one that capable of discussing the operation of transmissive control through algorithms.

Perspective and Digital Information

Perspective refers to how demons read packets, based on information stored in their memory. Demons can *read* packets during transmission because they are both encoded as digital information. Where past media have no understanding of the content of the conversation, the Internet protocol encodes all data digitally and embeds metadata about the content of the packet. Demons reads this metadata form instructions about the content and routing instructions of the packet. That any type of information – sound, video or text – could pass through the Internet depends on certain assumptions of digital information. These assumptions – specifically the decontextualization of information – allow demons greater sentience and autonomy in comparison to older media demons. A little history here aids in describing the awareness of demons.

Internet packets are digital variables: information[6] encoded into generic containers of bits. The digital variable is a very distinct form of encoding information particularly when compared to the printed word or the analog signal. Carpo (2011), in his history of architecture,

[6] Cybernetics and information theory have a particular understanding of information, not a conceptual replacement of Simondon. Mackenzie stresses that "Simondon's notion of information acts as a countermeasure to the tendency of recent cybernetic and biotechnological understandings of information to collapse living and non-living processes together" (2002, p. 52). The argument as follows remembers that *in-formation* is a way to understand the processes spawning from information theory and cybernetics. The two usages of the term are distinct.

offers a way to understand the encoding of the digital variable from prior forms of information encoding – a trend from "the ages of hand-making, of mechanical making and of digital making" (2011, p. 11). The first shift transpires under architect Leon Battista Alberti who encouraged architects to move from autographic production ("handmade by authors") to allographic production ("scripted by their authors in order to be materially executed by others") (Carpo, 2011, p. 16). Architect's blueprints, instead of their hands, guided construction. The allographic production is usually mechanical: the capability of reproducing fixed forms of information. The telephone, for example, is a form of allographic reproduction. It reproduces an analog of the voice as electric sound waves. A distant voice carried from one receiver to another depends on specific, relatively fixed systems that differ greatly from the nuances of a hand-written or autographic letter. Digital media blend the two; it is at once generic as in allographic production and specific as in autographic production. Carpo uses the example of changes in the authenticity of currency to illustrate its malleability. Financial transactions moved from bank notes to rather generic credit cards where "the validity of the credit card depends almost exclusively on a unique string of sixteen digits that identifies it" because "exactly transmissible but invisible algorithms have already replaced all visual and physical traces of authenticity" (Carpo, 2011, p. 4). The banknote depends on a mechanical production and reproduction that creates physically unique objects that signify, whereas a credit card is a variable sequence of numbers validated by algorithms developed by credit cards firms. While Carpo focuses on the notion of the author in relation to the digital, the difference also includes a distinct communicability of information. The digital represents the encoding of communication as a variable – a generic container for unique data (Robinson, 2008) – that depends on algorithms for its transmission and interpretation. Variable ontology acquires a much more specific meaning since it is a reference to the concept of a variable rather than the

term variance. Information, in the cybernetic sense, contains unique content that exists within a generic variable. Variables can be copied and transmitted constantly in a way of mass production while still being considered distinct through algorithmic processing.

Variability allowed the computers to encode older media. Streams of ones and zeros could contain voice conversations, binary files and data files. Digital systems could transmit everything as numerical representation, according to Manovich (2002, pp. 27–30), allowing older media to converge with the Internet. As Kittler writes,

> And if the optical fiber network reduces all formerly separate data flows to one standardized digital series of numbers, any medium can be translated into another. With numbers nothing is impossible. Modulation, transformation, synchronization; delay, memory, transposition; scrambling, scanning, mapping – a total connection of all media on a digital base erases the notion of the medium itself, (Kittler quoted in Johnston, 1999, p. 46)

Fibre optic networks re-mediate media because digital information separated information from its medium – printed word or sound wave – and converted it into bits of digital information. These conditions of digital information, far from being immaterial, illustrate how digital encoding include certain conditions of the medium and its materiality. Hayles states that "for information to exist, it must always be instantiated in a medium" (1999, p. 13). Variabilities, in fact, required a medium with set assumptions about the nature and content of information.

The belief that any data could be encoded as a variable and be separated from its medium depends on principles developed in cybernetics and information theory (Shannon & Weaver, 1949; Wiener, 1948). These theories, honed by scientists over America's scientific campaign during World War Two, reduced information to a pattern separate from its medium. Any message, any form of human or non-human communication, was a finite amount of disem-

bodied information. Information, to extrapolate, was simply a unit of knowledge – lacking any connection to meaning, context or material. This detachment was not an oversight. Separating information from its context or material was a compromise designed to ease its transmission. This was a controversial decision as seen in its criticisms by British researcher Donald Mackay who proposed that information theory needed to include how a receiver interprets a message – an element excluded from the cybernetic model (Hayles, 1999, pp. 50–57). "Shannon and Weiner define information in terms of what it is," Hayles states and, "Mackay defines it in terms of what it does" (1999, p. 56). His proposal met resistance for its degree of difficulty to mathematically model. Eventually, the mathematically simpler information model became the industrial standard in the United States. The decontextualization of information facilitated digitizing communication. Computer scientists and electrical engineers could focus on transmitting discrete units of information with mathematical precision and ignore the complexities of human context or even its physical medium. Delivery could be scientifically controlled – a link from warfare as firing messages or bullets both require mathematical formulas to ensure their effective delivery (Edwards, 1997) – to eliminate noise and to ensure a clear signal between sender and receiver.

Early ARPA engineers confronted decontextualization as a technical problem that they solved by layering the packet. Engineers buffered the particularities of a material from the actual communication. The physical actually became a layer, one of many, in ARPA's vision of packet switching. Ethernet, telephone lines and cables lines all could route packets if mediated by custom-encoded protocols to route information (Dennis, 2002, pp. 11–20). One of the first implementations of ARPA packet switching, AlohaNet, used radio to send packets (Kleinrock, 2010, p. 33). Separating link from application certainly aided in this application since the programmers only needed to adapt the link layer software. New applications also

benefitted from this separation because they could change how it operated, perhaps what information it sent, without changing some of the lower layers concerned with transmitting messages over various media.

Internet packets had to include a great deal of control information with the message itself to facilitate this separation of information from context. This allowed for an autonomy of the network previously impossible. Consider how transmissive control in the Strowger system works to automate telephone switching operated through a series of distinct wires to send control signals from the home to a central switching office, as seen in Figure 7.

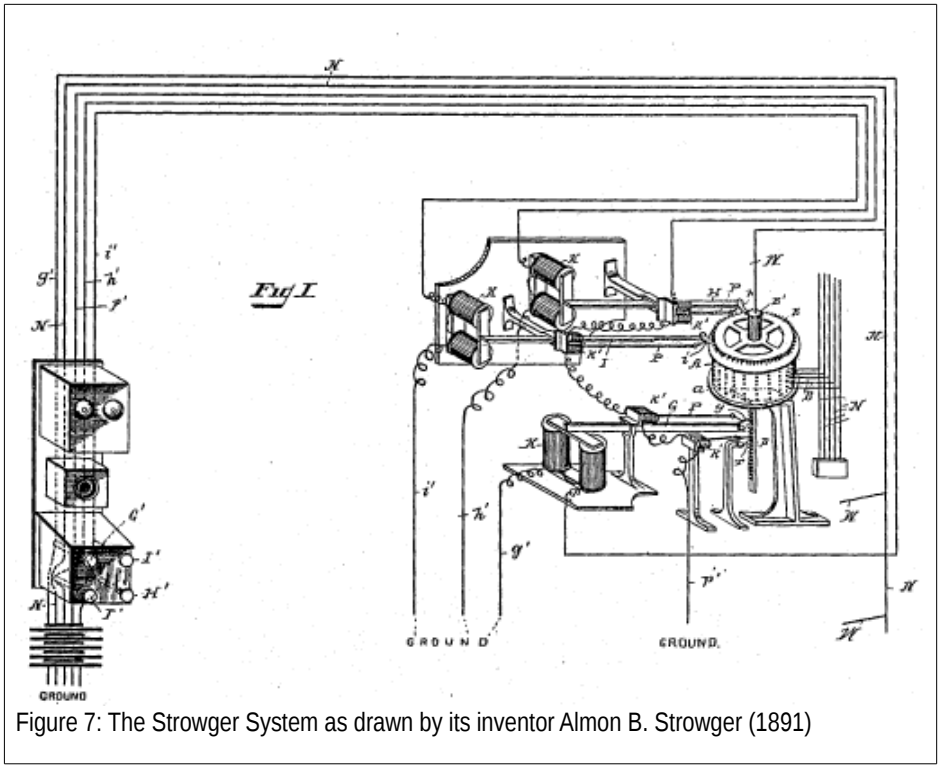


Figure 7: The Strowger System as drawn by its inventor Almon B. Strowger (1891)

A person from their home would press a series of buttons. These buttons would send an electrical pulse down specific lines. As its inventor Almon B. Strowger writes in his patent,

> the person wishing to place his transmitter and earphone in connection with those of another, he will do so by successively pressing or depressing the keys... For

> example, if telephone 288 wishes to place himself in connection with telephone 315 he will do so by pressing the key marked G'· three times, then the key marked II' once and then the key marked I' five times. (1891, p. 2)

Each pulse would be interpreted by an electro-mechanism to move a selector dial around a cylinder of potential connections. The programming on the selector dial travelled over separate lines than the actual message. The Internet, on the other hand, embedded information – like the destination of the message – into packet. All these locations and standards became codified in the Internet Protocol Suite (TCP/IP) that all demons read and route packets accordingly.

The perspective of a demon is almost entirely protocological (Galloway & Thacker, 2004). Standards, such as the thousands in the Request for Comments index (see Crocker, 2009), specify the significance of bits and the preliminary rules for response that become encoded in a demon's programming. Protocols provide instructions to comprehend a flow of bits. Most Internet demons pay close attention to the 65 to 96 bits of packets. As each bit in this segment arrives, the bits translate into numbers that, in turn, emerge as a destination address. The control information encapsulated in the packet allows demons to understand the context of a message. With this information, a demon can be said to understand a message and act upon it. To a demon, understanding involves simple pattern recognition whereby a demon compares a current string of bits to past strings of bits. Port numbers most clearly illustrate the linkage between a variable set of information and a means of demonic recognition. Exchanges between computers rely on port numbers to isolate flow specific to functions or applications. An ad-hoc list relates port numbers to applications. The list assigns Port 22, for example, to the File Transfer Protocol (FTP), where it assigns port 80 to the Hypertext Transfer Protocol (HTTP) data. Linking a port number to an application becomes a moment of understanding

for the demons where their memory remembers a class for a passing packet (Tanenbaum, 2002).

Demons use protocols as part of their profiling of traffic. Profiles are the memory of demons. Elmer (2004) introduces profiling to explain the algorithmic processes that build models for machine understanding of noisy and chaotic inputs. Profiling normalizes input to relate to past behaviour. Computers collect personal information to create machine-readable profiles that inform its decisions and its simulations. Elmer states that commercial profiling "oscillates between seemingly rewarding participation and punishing attempts to elect not to divulge personal information" (2004, p. 6) to create information systems that "place individual wants and desires into larger, rationalized and easily diagnosable profiles" (2004, p. 23). Where protocols offer a very intensive form of profiling, advanced traffic management algorithms use extensive profiling by logging traffic flows to build profiles of customer behaviours. Profiling not only applies to personal information though. Internet Service Providers aggregate usage data from their many installations to create profiles of traffic trends. Traffic profiles help demons manage bandwidth and identify threats. Using port numbers and IP addresses, the perspective of a demon hinges on the profiles built into their memory. Profiles assign a packet a past that eases its demons processing of the information. Since digital information separates the bits of a message from its context, the demon only needs to inspect bits of a message to make a decision. By connecting the packet to past models of traffic spikes, patterns of past attacks and conditions of service level agreements, they are able to control the transmission more effectively.

Packet switching, in summary, expresses messages as digital variables designed to be inputs for algorithmic processing. Carpo (2011) provides the example of the credit card number as one elementary variable. Even though the numbers of the card changes, it fits into a

variable container fed into verification and financial software. The human in the Internet is simply one variable among many. Packets encode communications as *flows* – to borrow a word from Castells (1996) – subject to the eternal repetitions of Internet demons. Demons do not attempt to discipline behaviour, but affects the transmission of behaviour indefinitely. As Deleuze states, "control is short-term and of rapid rates of turnover, but also continuous and without limit" (1992, p. 6). The user is not disciplined to stop future activity, rather, software merely repeats the same process of management for each time the users switches into discouraged activities. Continued transgressions limit users' allocated bandwidth or flag the user as a threat. Maybe, the user will learn and stop their transgressive activities, but control does not require their obedience. Dissent passes through the same filters and software throttles the flow of packets. Each malicious packet gets the same treatment as the next. Yet, how algorithms treat packets requires more attention. The next section then elaborates on the second characteristic of algorithms: programming.

Logics and Digital Programming

Profiles translate packets into inputs for demons to interpret according to their programming. How algorithms process this input defines networks since they assign and utilize finite network resources. 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. Do algorithms treat packets equally? Home computers might use peer-to-peer algorithms to share files, while servers could use queuing algorithms to manage bandwidth and routers may employ quality of service algorithms to prioritize packets. What logics are at work? Some logics might prioritize some packets to ensure their fast and lossless delivery at the expense of other packets that must receive fewer resources.

The existence of many logics on the Internet is a result of decision made at the inception of the Internet to embed intelligence in the network. Packet switching depended on demons to assist in encoding, transmitting and decoding digital messages. One of the developers of ARPANET Leonard Kleinrock, in his history of the Internet, cites their task as two-fold: creating protocols and creating the computers with the software to actually run the protocols (Kleinrock, 2010, p. 29). Kleinrock writes, "the ability to introduce new programs, new functions, new topologies, new nodes, etc., are all enhanced by the programmable features of a clever communications processor/multiplexor at the software node" (1978a, p. 1328). Cleverness, in short, meant including computers that were *programmable* or capable of obeying set instructions (see Chun, 2008). Digital computers could have their programming changed. One of the first initiatives of the ARPANET project was to contract the firm Bolt, Beranek and Newman to modify Honeywell DDP-516 minicomputers to transmit computer messages, also known as an Interface Message Processor (IMP) (Kleinrock, 2010, p. 30). IMPs facilitated packet routing and queues: tasks given to the early and oldest demons of the Internet. The IMP opened the network to the demons waiting at its gates. Soon demons infested computer networks and enthralled engineers and administrators who soon made use of their uncanny services. Network administrators realized they could program software demons to carry menial and repetitive tasks – often dull, but essential to the network operation.

By building their network control using computers, ARPA switched from then-conventional analog programming to digital programming. The switch expands the kinds of demons controlling transmission because digital programming is more dynamic than analog programming. Programming refers to "physically encoded information" (Beniger, 1986, p. 40). While Beniger (1986) argues programmed control existed since the late 1800s, there is a shift in its constitution from analog to digital systems. The metal and wood components of the Strowger

switch exemplify an analog programming. The early Strowger switching station "consists basically of selector arms moving in front of contact banks" (Huurdeman, 2003, p. 196). Control was physically encoded in the range of the selector arm and how it moved across the selector banks. Where programming in an analog machine requires physical mechanical components, digital programming simply alters the bits in an electronic memory bank. Digital computers involves a kind of programming, to borrow from Kittler (1995), that does "not exist anymore in perceivable time and space but in a computer memory's transistor cells" (np). Computer scientists sold digital computing, as Edwards makes clear in his discussion of the contingent development of digital computer, on the promise of re-programmable control system. One of the first digital computers, Whirlwind, secured the defence funding with the promise of being a general simulator for training, a huge savings considering pilots and others often trained on physical, analog simulators of aircrafts (1997, pp. 76–81). Once built, an electronic system provided reprogrammable control since its electronic programming could change without physically changing the system.

The switch to the digital alters the retention of programming or how the effect of control repeats (See Stiegler, 1998, p. 25, 2010). A mechanical part repeats because its form embodies control. The being of mechanical control is no more or less than its function. This control is often defined as analog because it depends on a continuous signal – the whole of the part (Manovich, 2002, pp. 27–30). Engineers programmed control into intricate, but also battle-tested, machines using physical knobs, circuits, diodes and transistors. Computers, conversely, could be easily programmed by altering the instructions stored in their memory, allowing computers to run variable instructions or software (Ceruzzi, 1998, pp. 79–108). Programming shifts from a tangible physical object to the electronic manipulation of an electric current. Since the being of a digital system is ephemeral, not physical, the nature of control

becomes much more malleable. The retention of a program relies on encoding on a magnetic disk or solid-state drive. This comes at a cost of durability and permanence, yet allows for near instantaneous re-programming and high adaptability to its inputs.

Digital programming allows thousands of different kinds of algorithms that change and can be updated. Home computers might use peer-to-peer algorithms to share files, where servers could use queuing algorithms to mange bandwidth and routers may employ quality of service algorithms to prioritize packets. These decisions relate to a demon's vision of a network. Most Internet routing hardware allow administrators access to their programming. In fact, the two major manufacturers, Cisco Systems and Juniper Networks, both have developed operating systems to allow network administrators to program complex instructions into their routing devices (Duffy, 2007a). More recently, a whole industry has developed providing complex, highly configurable traffic management appliances capable of being configured and programming to target and manage specific kinds of Internet traffic as demonstrated by ComCast (Bendrath & Mueller, 2011; Finnie, 2009). Since these appliances can understand the messages routing through their networks, they have an unprecedented ability to control the rate of transmission of different kinds of transmission, such as peer-to-peer.

Algorithms have a few different ways to control the rate of transmission. Algorithmic logics entail certain ways of transmitting packets. Logics process packets in many different ways, but they have four major forms of control over transmission. They can control the rate of transmission by effecting jitter (the variation in packet arrival times), reliability (the level of error in transmission), delay or latency (the time to receive a response to a request) and bandwidth (the rate the ones and zeros or bits of an application pass over a network, usually measured per second as in 10 Megabytes per second) (Tanenbaum, 2002, pp. 397–408). Logics seek to direct traffic toward particular idealized forms of networking, such as home computers and

peer-to-peer networking to create a decentralized network or where privileging the network to centralize servers and infrastructure. Encoded in their loops and cycles is a sense of an ideal network that it processes information toward. The forms become the future goals that algorithms enact when processing information. How algorithms process packets, in other words, creates processes of networking.

Many kinds of algorithms have spawned from these mutable origins. Computer Science refers to the differences of algorithms as a matter of *time complexity* (Mackenzie, 2007). The concept refers to the amount of time required by an algorithm to process an input. The theory of time complexity in Computer Science acknowledges that different algorithms have different *running times* based on the steps it takes to process an input. It is a way of considering the duration of an algorithm – how the algorithms passes through time. Algorithms and programming language differ in their time requirements and thereby time complexity (Sipser, 2006, chap. 7). While these might be debate about the capacity to compare durations between Bergson and Computer Science, the link clearly demonstrates that computing time depends on certain conditions of the algorithms. These conditions play an important part in the routing of information as the time complexity of an algorithms impacts how it might transmit and modulate its rates of transmission.

The Living Present

Perspective and logic then become the two components of transmissive control. Profiling and logics function respectively as a past and future that synthesize at the moment of transmission. The duration of a packet passing through a network varies by how demons integrate pasts and futures to constitute the passing of the living present. Linking a packet to a profile assigns the profile a past – a past that might regard the packet as a threat based on past traffic

or as an integrated service. The memory of a router includes all these profiles and protocols built from past traffic. The past comes from machine-readable profiles derived from monitoring techniques within networks that inspect traffic to build models or simulations of the modalities of traffic, its risks and its costs (Elmer, 2004). At the same moment, the past links with a history – a future for the packet. The logic of networking is the future of the packet, the goal of what a network should be. Routing according to a networking logic integrates a future goal into the passage of a packet in a network. The future remains a desired network form (Latham, 2005) that algorithms work toward by "increasing the probability of a desired outcome rather than its absolute determination" (Samarajiva, 1996, p. 129). Transmissive control software invokes pasts from profiles and futures from programmed goals to actualize presents. Packets experience different passages of a specific duration depending on how the software relates the contents of the packet to a profile and how the software treats the identified profile. Patterns in these durations create temporalities on the Internet.

The living present is not pure difference, but a *modulation* that varies by profiling and logics of demons. Time complexity is central to understand the dynamics of modulation. Different algorithms can do more or less in a cycle of computing. Their difference in time complexity is a difference in modulation. The modulations of transmission narrow or widen according to its algorithms. Time complexity – what are they able to accomplish in a computing cycle – refers to the modulation of an algorithm. How are they able to create different rates of transmission? How many can they hold in a system of relations? How fast might an algorithm respond to a change in input? How granular can the input of an algorithm be? These questions will become more apparent in the following discussion of Internet routing algorithms, but it is important to remember that modulation depends on the capacity of the

algorithm and, as will be seen, new traffic management algorithms rapidly increase the modulation of transmissive control.

The modulation of algorithms creates patterns in transmission that express temporalities. What algorithms become part of a communication system influence the kinds of temporalities that can be expressed. Temporal economies differ in their machinic assemblage of algorithms and these algorithms enact transmissive control in various ways. Most Internet algorithms modulate enough to create an asynchronous temporality. These algorithms, generally known as ones operating according to the End-to-End principle will be discussed in detail in the following section. New traffic management algorithms or Quality of Service have a different modulation allowing for a *poly-chronous* temporality. The following section discusses these two kinds of algorithms, their temporalities and the conflicts between them.

Pandemonium: The Internet as a Place of Demons

Mean while the winged Haralds by command

Of Sovran power, with awful Ceremony

And Trumpets sound throughout the Host proclaim

A solemn Councel forthwith to be held

At Pandæmonium, the high Capital

Of Satan and his Peers: thir summons call'd

From every Band and squared Regiment

By place or choice the worthiest; they anon

With hunderds and with thousands trooping came

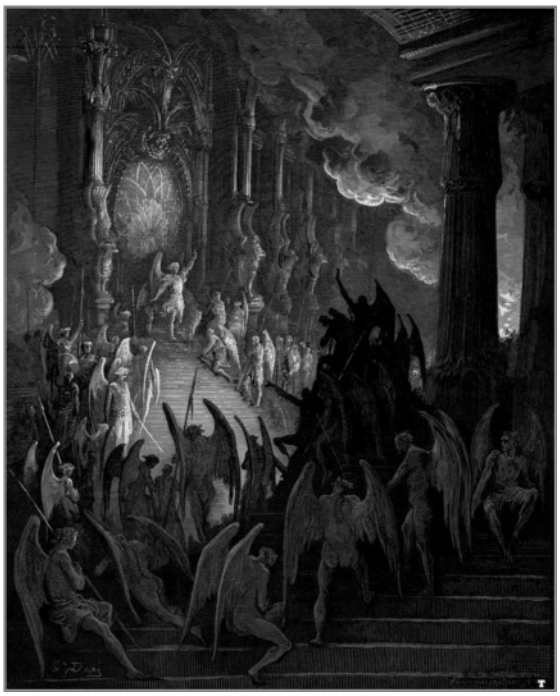


Figure 8: Satan addressing the demons of Pandemonium, woodcut by Gustave Doré

One of the founders of artificial intelligence, Oliver Selfridge, saw software as orchestrations of demons. In his description of a language-recognition program, he described each of the algorithms recognizing individual letters as demons. Perhaps Selfridge's infatuations with demons started when he worked as a research assistant for Norbert Wiener (Crevier, 1993, pp. 40–41). Independent demons, he explained, would each learn to recognize letters and their cooperation would be able to interpret words. It works as a demon that "computes a shriek and from all the shrieks the highest level demon of all, the decision demon, merely selects the loudest" (Selfridge, 1959, p. 516). All this noise inspired Selfridge to name his program Pandemonium – the name for the Capital of Hell and a place full of demons in poet Milton's Para-

dise Lost. "Selfridge believed an AI program should look like Milton's capital of Hell: a screaming chorus of demons, all yelling their decisions to a master decision-making demon" (Crevier, 1993, p. 40). The decision demon would select the loudest yell as probably the right choice of letter corresponding to the inputed pattern. If Pandemonium is the product of the collaboration of demons, then what is the Pandemonium of the transmissive control online?

The Internet as Pandemonium is a vast capital with many floors that, in reality, correspond to the conceptual layers of network employed by engineers and administrators. The Open Systems Interconnection (OSI) standards is the most common model of layering. It offers network architects and engineers seven layers to guide connecting switches to hubs to, eventually, home computers. Higher layers have more sentience and authority. The first two layers, Layer 1 - Physical and Layer 2 - Datalink, ensure "transmitting data bits (zeros or ones) over a communication circuit" (Dennis, 2002, p. 16). Rising the stack, Layer 3 - Network and Layer 4 - Transport, coordinate the lower layers to create networks. The TCP and IP protocols function at this layer. Where Layer 1 or Layer 2 devices, such as a hub or a repeater, simply send packets further along the network, Layer 3 devices, such as a switch or a router, make choices as to how best to route a packet to get it closer to its destination. Finally, the last three layers, Layer 5 - Session, Layer 6 - Presentation and Layer 7 - Application, host software using the network. Home computers fall within these layers (Dennis, 2002, pp. 13–20,141–146). For Pandemonium, the higher the floor of a demon, the more intelligent and the more weight their opinion has among the other demons. The lower demons, while interesting, do little other than carry out orders of higher demons – blindly passing messages from sender to receiver.

The current asynchronous Internet as an assemblage of demons resembles the popular usage of Pandemonium. The Oxford English Dictionary defines it as "a place or state of utter confusion and uproar; a noisy disorderly place". Without a centralized control, demons create

all sorts of temporalities. Congestion and capacity issues plague this Internet. The noise and confusion have caused a new breed to demon to emerge, one that seeks to create order out of the multitude of transmissions online. Quality of Service algorithms, as will be discussed, promise to enhance their modulations of the transmissive control to override the orders of older end-to end demons. This conflict within the very nature of transmission on the Internet helps explain what is new about transmissive control enable by advanced traffic management software with its Quality of Service demons.

Asynchronicity and End-to-End Demons

The oldest demons of the Internet are *end-to-end* (E2E) algorithms that facilitate the asynchronous communication of the Internet. Jerome Saltzer, David Reed and David Clark formalized the term in 1984 (Gillespie, 2006b). In a seminal article entitled *End-to-End Arguments in System Design,* they outlined a design principle for computer engineers to follow when developing data communications networks. It prioritizes the endpoints, the sender and the receiver, of the network in order to ensure proper communication of messages. It 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, p. 287). Only the sender and the receiver can guarantee the accuracy of a message because they alone know its contents. E2E celebrated the *stupid network* where the network did little else than carry bits between the ends (Isenberg, 1998). Thus, a packet passing through this spire would enter at great heights and then plummet as lower level demons mindlessly pass it through the depths of networks and then quickly hoist it up to the higher floors as it exits at its destination. The E2E spire lowers the importance of the

actual network and raises the ends of the network to do most of the work in sending and receiving packets.

It would be unfair, though, to call the demons of the Internet stupid because E2E requires significant intelligence of the network to route packets on to their destination. Routing is a complex operation on the Internet because its protocols commonly utilize a connectionless model of communication where the network does not establish a unique connection between two nodes. Packets travel along common paths. A router has to be aware enough to know its connections by keeping a dynamic routing table, a simple network logic, which remembers its connections and the best direction to send a packet toward its destination.

Demons route packets by reading the upper layers of a packet. The TCP/IP packet datagram, as mentioned earlier, contains four nested layers, a version of the OSI model. The first three layers contain information about the transportation of a packet over a network and the last layer contains a header and parts of the message. The higher-level bits arrive sooner and contain routing information. Its design eases the perspective of the demon, which quickly reads the destination, looks up the best route in memory and sends the packet on its way. Their perspective also overlooks the actual content of message, relaying only the information in the upper layers (Dennis, 2002, pp. 13–20). In this way, only the ends have real control over setting the tempo the Internet.

E2E network demons must also be smart enough to handle the deluge of packets arriving at its networks. To handle floods of packets, demons queue and store packets before forwarding them to their next destination; for this reason, packet switching is also called *store-and-forward* (see Kleinrock, 1978a). Leonard Kleinrock, one of the scientists that would work at ARPA on the packet switching, wrote his dissertation on a mathematical theory for effective queuing to prevent congestion and ensure efficient resource allocation (Kleinrock, 2010, pp.

26–28). He continued to develop programs "to throttle the flow of traffic entering (and leaving) the net in a way which protects the network and the data sources from each other while at the same time maintaining a smooth flow of data in an efficient fashion" (Kleinrock, 1978b, p. 1). Much of the early work on the ARPANET included testing methods of flow control. Flow control proved difficult often leading to deadlocks or failures in ARPA (Kleinrock, 1978a, pp. 1324–1325). Eventually, they settled on a Best- Efforts approach after considering a few different options.

The Best Efforts approach took a radical step by privileging the ends of a communication system. ARPANET initially preferred active network management – a virtual circuit – where the network managed communication enough to ensure its safe delivery. Their approached 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 the "isolated islands" of computer networks (Abbate, 1999, p. 124). It championed less involvement of the core of the network and greater responsibility at the ends. The network, as a result, could not ensure the delivery of packet, rather, software did its best effort to route packets safely and left message control at the ends of the network. Stupid networks proved easier to implement and expands, a reality that ARPA accepted and implemented in their own protocols (Kleinrock, 2010, pp. 34–35). Best efforts amounts to a network doing "its best to deliver datagrams"; however, "it does not provide any guarantees regarding delays, bandwidth or losses" (Van Schewick, 2010, p. 85). Since networks can be overwhelmed, flow control stipulated that packets would be dropped, forcing a node to re-send the packets at a more opportune time. Best-efforts algorithms, over time, became the de-facto standard with the articulation of the end-to-end principle and the stabilization of Internet Protocol Suite (TCP/IP).

A typical E2E demon at the home computer would be an application running on the home computer. Consider browsing the web as an example one bevy of demons. As "readers 'follow' links (by clicking them) to create their own 'paths' or 'trails' through the connected documents" (Kirschenbaum, 2000, p. 120). Underlying this experience of links and connections are high-level demons packaging clicks as HTTP request packets, sending them along the network to the web server that interprets the request and sends an HTTP response packets. While layer-3 demons at the core of the network transports the HTTP packets, it leaves the important decisions to the browser and the web (Dennis, 2002, pp. 42–45). Packet moving from end-to-end spend most their time on the third floor with demons that reside on gateways, routers or switches. The presence of demons can be felt because "most routers introduce a small but noticeable delay in moving one network to another" because they introduce software into the transmission of packets (Dennis, 2002, pp. 143–144). These aspects define the range of modulation by E2E algorithms.

E2E expresses an *asynchronous* temporal economy by allowing the ends to set the rates of transmission. Temporalities occur at the discretion of the demons at the ends. Demons may agree to create decentralized networks or personal communications between nodes. A symmetry exists within the economy as the ends have mutually agreed to participate in a temporality. Ends have some degree of authority when expressing their common temporality. Many Internet legal scholars argue the symmetry of E2E fosters innovation and user-led development (Benkler, 2006; Van Schewick, 2010; Zittrain, 2008). Since the ends have the bulk of the authority over transmitting messages, they can innovate new ways of transmission. Zittrain goes so far as to refer to this as the *generative web*. He explains, "the end-to-end argument stands for modularity in network design: it allows the network nerds, both protocol designers and ISP implementers, to do their work without giving a thought to network hardware or PC

software" and continues that aspects of E2E invite "others to overcome the network's shortcomings, and to continue adding to its uses" (2008, p. 31). Zittrain, as well as both Benkler and Van Schewick, attribute core innovations, like the World Wide Web, to E2E as any end could contribute to the network functionality.

Asynchronicity does not, however, have one version as Van Schewick suggests E2E bifurcated into a broad and narrow versions. The narrow version comes from the original 1984 article and "provides two design rules for end-to-end functions: first, end-to-end functions must be implemented at a layer where they can be completely and correctly implemented. Second, whether the function should also be implemented at a lower layer must be decided case by case" (Van Schewick, 2010, pp. 60–61). The narrow definition allows for the demons of the core network to ascend to higher floors so they can optimize network performance narrowing the gap in authority between the peaks of the ends and the ruts of the network. Error control demons between nodes in a network, for example, would have some network intelligence that fits with this version. The broad definition is a re-interpretation of the principle by the authors in an article from 1998. It states that "specific application-level functions usually cannot and preferably should not, be built into the lower levels of the system – the core of the network" (Reed, Saltzer, and Clark, quoted in Van Schewick, 2010, p. 67). Van Schewick points out that the two both compromise on network functionality. The design rules of the broad version, Van Schewick writes, "reflect the decision to prioritize long-term system evolvability, application autonomy and reliability over short-term performance optimizations" (Van Schewick, 2010, p. 79). They argue encoding functions in the core prevents the system from adapting because of cost and difficulty of changing core networking software; however, this flexibility comes at a cost of network performance since the network is intelligent enough to optimize traffic and control for errors. The network has less intelligence,

but more adaptability. The difference between the two concerns the evolution of the network. Building higher functionality in the core alters network innovation, a central point for Van Schewick. Greater intelligence in the core empowers administrators to guide innovation, where a broad end-to-end argument impedes core innovation at the core to ensure the network adjusts to the innovation at the ends.

If differences exist between the broad and narrow versions of E2E, then P2P further deviates by privileging the equality of the ends absolutely. Peer-to-peer is a class of application that treats all interconnecting nodes as equal peers and removes the need for a certain server. P2P as the extreme version of E2E attempts to create an even more extreme version of *asynchronicity* – almost an *isochronous* temporality – that seeks to create equality between nodes. These P2P demons have arisen after generations of advocates of Internet free speech pushed the implications of E2E principle even further (Gillespie, 2006b; Sandvig, 2006). The ends of the network, proponents argued, must be free without the impositions of centralized control. Nethead John Perry Barlow, for example, once quipped, "the Internet treats censorship as a malfunction and routes around it". "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" (Gillespie, 2006b, p. 443). Recursive publics of P2P, as discussed, produce new kinds of algorithms forever trying to increase the decentralization of their networks (Dyer-Witheford, 2002; Oram, 2001; Wu, 2003b). P2P demons, high above at the ends, encourage multiple sessions since their logics consider every end a productive part. Their networking expands laterally between ends that upload and download bits without concern for hubs or centres. Network congestion is a result of P2P network relations. Its algorithms ignore their demands on a network, instead, of the message to preserve the equal

treatment of all packets and to prioritize the ends of the network. The arrogance of P2P demons has not gone unnoticed by lower-level demons that have suffered in their service.

E2E has fallen into decay in recent times. A lack of a clear vision and central authority caused its Pandemonium to be chaotic and error-prone. Further, the antagonism of P2P to core network demons has chaffed and coaxed them to build a new spire. They have conspired to manifest their logics into new networks capable of usurping E2E. These demons sought to override the transmissive control of demons at the end with their own control. It promises to pass the heights of peaks of the E2E spire. This spire is known as Quality of Service (QoS). It is a tower that has evolved along with the propagation of new network demons. Quality of Service raises the core above the humble third floor; it grants the network dominion over bandwidth to ensure certain channels of communication receive sufficient resources to guarantee their successful operation. If a conflict exists in the network, then Quality of Service seeks to have greater say in the production and assignment of temporalities of transmission.

Poly-chronicity and Quality of Service

Quality of Service originated in the telecommunications industry (Mansell, 1993) with its *instant world* temporal economy. It has guaranteed levels of service in response to the contractual obligations of the customer in an era of public service (Crawford, 2006, 2007; Gillespie, 2006b). 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, pp. 241–243). This perspective differs from 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 Cir-

cuits 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 this model as the best way to ensure reliable communication online and to optimize networks for time-sensitive applications such as voice conversations (Gillespie, 2006b, pp. 431–435).

Most often, management adheres to Quality of Service due to the contractual obligations place between customers and their ISPs which 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 network capable of being able to make decisions about the value of a packet. 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, p. 568). QoS, in sum, intervenes in E2E exchanges to manage scarce bandwidth by prioritizing and de-prioritizing packets – in effect, overriding asynchronicity.

The Internet, initially, featured fairly unsophisticated demons in the core that could not abide by the tradition of Quality of Service. Brutish and ill-mannered, they could not rise to greater levels. The Internet Protocol did contain provisions for QoS, but implementation was optional. 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 networks. Gradually, network administrators found the need to conjure more mannered demons in the networks. New breeds of demons came from many sources. Developments in networking

around security, congestion and multimedia all offered demons a chance to refine themselves. These three technologies gradually raised demons high into the upper floors of Pandemonium.

Firewalls were one of the first introductions of intelligent demons in the core of the network. Firewalls responded to the problem of the Internet to corporate networks. According to Bill Cheswick and Steven Bellovin, two former members of Bell Labs who were among the first to write about Internet security, "networks expose computers to the problem of transitive trust. Your computers may be secure, but you may have users who connect from other machines that are less secure" (1994, p. 50). While the Internet could simply be shut off, a more nuanced problem emerged as networks sought to stay connected, but remain secure. Firewalls offered a compromise because "there are no absolutes. One cannot have complete safety; to pursue that chimera is to ignore the costs of the pursuit. Networks and internetworks have advantages; to disconnect from a network is to deny oneself those advantages" (Bellovin & Cheswick, 1994, p. 50). Cheswick and Bellovin suggested securing network connections by installing filtering software called firewalls. The term comes from car design where *firewalls* protected passengers in the cab from engine fires. The same logic applied to networks as administrators installed software to buffer their users from outside threats by selectively allowing and denying the entry of packets into a network according to simple rules. While firewalls had been around for some time,a self-replicating computer program known as the Morris Worm appeared on networks beginning on 2 November 1988. The worm's buggy code devastated networks and sent their administrators scrambling. The worm popularized the usage of firewalls – hoping to stop such an attacks in the future (Orman, 2003). Beginning in the later 1980s and early 1990s, networks started to employ firewalls to protect their internal

networks. With the delivery of the first commercial firewall on 13 June 1991 by Digital Equipment Corporation, came packet filtering and firewall demons into the network (Avolio, 1999).

At the same time of the rise of firewalls, networks also came to require greater management. NSFNET and other major computer networks suffered from severe congestion in the early 1990s (Abbate, 2010, pp. 12–15). Controlling the flow of packets vexed even the earliest network researchers (see Kleinrock, 1978a). A number of queuing algorithms other than best efforts attempted to solve the problem. They included Random Early Detection (RED) and active queue management (AQM) (Welzl, 2005, pp. 26–28). Flow control began with a sense that different users and application had different requirements for the network. Even the strict version of E2E acknowledged a difference between data and voice communications[7]. Quality of Service has the following requirements: jitter (the variation in packet arrival times), reliability (the level of error in transmission), delay (the time to receive a response to a request) and bandwidth (the rate the ones and zeros or bits of an application pass over a network, usually measured per second as in 10 Megabytes per second) (Tanenbaum, 2002, pp. 397–408). Crucially, all these characteristics involve a modulation of the duration of a packet within a network and in QoS, this modulation is deliberate, such that the network seeks to control jitter or bandwidth for specific applications or users. Given the importance of flow control, it is worth exploring its perspective and program more in depth.

QoS demons have a better memory or sense of the past in their operations. Without mixing metaphors too much, the technical literature describes flow control and its relation to

[7] Salter, Reed, & Clark thought E2E could easily handle voice communication given that "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).

Quality of Service through the concept of buckets. The two buckets manifest in the network as specific algorithms of packet queuing. The leaky bucket, first used by Turner (1986), depicts the flow of packets as drips of water from a bucket. The bucket fills with packets from hosts on its networks and empties as the packets drip from its leak. The bucket acts as a metaphor for a finite packet queue. For engineers, when the queue fills, the network begins to drop packets.

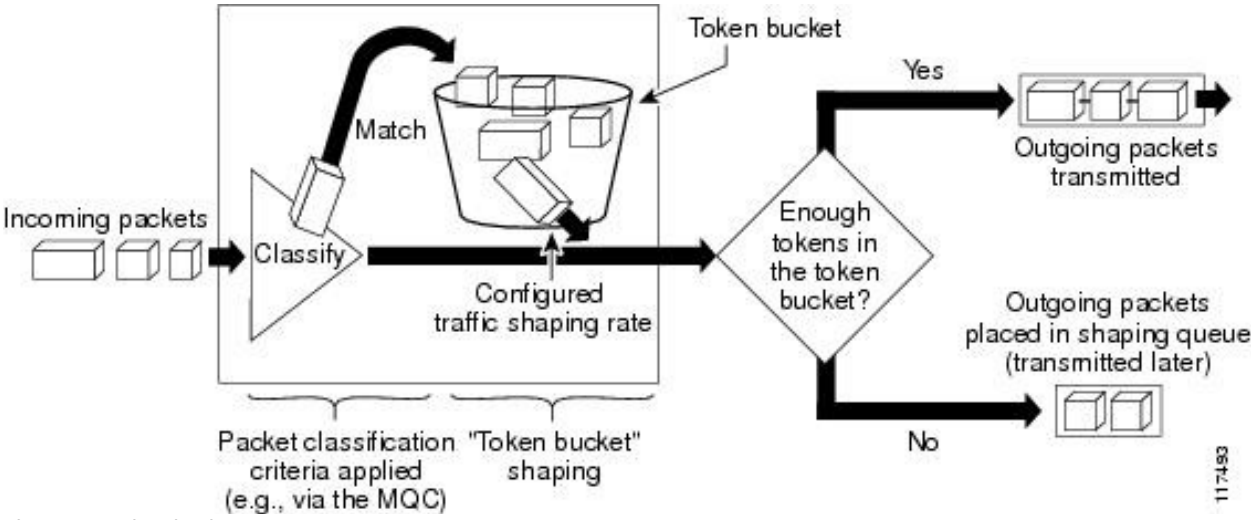


Figure 9: A token bucket

The leaky bucket inspired another model, the token bucket, as depicted in a diagram by Cisco seen Figure 9 (Cisco Systems, 2005, p. QC–34). For a host to send a packet, it must spend a token. Hosts gradually build up tokens as they remain on the network until the bucket fills with tokens and a system stops handing out tokens. Thus, the algorithms differ in that "the token bucket algorithm throws away tokens (i.e., transmission capacity) when the bucket fills up but never discards packets. In contrast, the leaky bucket algorithm discards packets when the bucket fills up" (Tanenbaum, 2002, p. 402). Most current forms of traffic management

assign priority to packets in queues, according to these buckets or other algorithms, so that some packets languish in queues where others cut to the front of the line.

Flow control also concerns ensuring application traffic has the sufficient bandwidth to function correctly. Bandwidth is a major concern for multimedia applications. With the convergence of the Internet, great efforts were taken to improve routing of multimedia. The Internet Engineering Task Force invested heavily in providing multimedia service online by developing new networking logics other than best efforts. The research produced a number of Request for Comments (the means to publicize and to implement new features online). RFC 2205, released in 1997, outlines the Resource reSerVation Protocol (RSVP) that outlines a means for the ends to communicate with networks to reserve a path and resources among networks. It provided the foundation for the Differentiated Services (DiffServ) QoS networing logic, outlined in RFCs 2474, 2475 (Tanenbaum, 2002, pp. 409–411). DiffServ built on its predecessor Integrated Services that "represented an important modification of the traditional Internet paradigm" because "the responsibility to maintain flow information is distributed to all nodes along the network" (Ibarrola, Liberal, & Ferro, 2010, p. 17). Using DiffServ, networks assigns packets to classes based on the Type of Service specified in their header and routes these packets according to the priority of the class. No matter the context or instance of a Type of Service, the network will route these packets according to its QoS policies (Tanenbaum, 2002, pp. 412–414). Classes, then, become a way for network demons to widen their enforcement of Quality of Service without needing to enlist other networks.

Though DiffServ demons continue to inform QoS models, the IETF in collaboration with Cisco and Juniper Networks, the two dominant networking infrastructure vendors, developed MultiProtocol Label Switching (Paterson, 2009, pp. 185–189; Tanenbaum, 2002, pp. 415–417). RFC 3031, released in 2001, outlines a system with which to label packets entering a

network. The label travels with the packet through the network, so that subsequent layers in the network need only read the MPLS label to decide their task (Rosen, Viswanathan, & Callon, 2001). The label rests before the IP and TCP data in the bitstream of a packet and includes a label, a QoS field that specifies the class of service, a stack label for complex service layering and the conventional Time-to-Live (TTL) that specifics how long a packet endures on a network before being discarded. The labels bypass the Internet headers, allowing as Tenanbaum describes as something "perilously close to virtual circuits – tiered networks that rapidly delineate traffic and routes" (Tanenbaum, 2002, p. 415). It has risen to be one of the most popular forms of Quality of Service online, widely implemented in Internet backbone networks since late 2002(Paterson, 2009, p. 186).

Firewalls, congestion and multimedia provoked an increase in the intelligence of core network demons. Further competition in networking infrastructure industry led to rapid advances in QoS algorithms. By the late 1990s, Cisco Systems (started in 1987) and Juniper Networks (founded in 1996) emerged as the two dominant players in the field. Each competed through advances in the computational capacity of their products and in the sophistication of the networking operating systems installed on most routers. Cisco developed IOS, where Juniper wrote JUNOS (Duffy, 2007a). Each allowed network administrators to program routers to process packets according to built-in commands such as *police* or *shape* (Duffy, 2007b). Newer versions also implemented QoS models such as DiffServ and different forms of queuing. RSVP, for instance, arrived in Cisco IOS 11.1CC, a version of IOS released in 1998 (Cisco Systems, 2002). The advances allowed these processors to route packets and, simultaneously, manage packets using queues, shaping and policing. A brochure for the Cisco CRS-1 router, the firm's largest router when it launched in 2004 that boasts providing "total separation of traffic and network operations on a per-service or per-customer basis" that allows "car-

riers to isolate the control, data and management planes" with the "confidence that they can meet customer service-level agreements" (Cisco Systems, 2009).

Growth in Internet usage, particularly file-sharing, has only amplified the need for QoS management. ISPs cite the growth in file-sharing and bandwidth-intensive applications as technical developments that have degraded their quality of service for their customers (McTaggart, 2008). 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 fuelled the influx of QoS demons (Finnie, 2009; Ingham & Forrest, 2006).

These factors led to a decision to augment E2E algorithms with ones with greater perspective and more sophisticated programming. In doing so, the modulations of transmissive control expanded to allow Internet Service Providers a more granular control over Internet traffic. Asynchronicity could now be managed as QoS algorithms could observe and intervene in traffic flows to override decisions at the ends. This capacity is most clear in the advent of two major new types of algorithms have facilitated the growth of QoS networking: Deep Packet Inspection (DPI) and deep flow inspection (DFI). These technologies greatly widen the modulation of temporality to the level of advanced transmissive control. They afford much greater perspective drawing on advanced profiles of the past as well as much more defined futures encoded as policies that aggregate traffic flows into classes and tiers. More than ever, these algorithms threaten to restructure the Pandemonium of the Internet.

The gaze of demons, however, sharpens considerably with DPI. As its name implies, DPI inspects 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. Its profiling has taken on greater importance because of a practice known as port-spoofing where an application sends its data on unconventional ports. BitTorrent applications, in an effort to avoid detection, send packets on HTTP ports rather than their standard ports. As Sandvine Corporation, a leading manufacturer of DPI software, writes:

> DPI is necessary for the identification of traffic today because the historically-used "honour-based" port system of application classification no longer works.
>
> Essentially, some application developers have either intentionally or unintentionally designed their applications to obfuscate the identity of the application. Today, DPI technology represents the only effective way to accurately identify different types of applications. (2009)

Even though a port may be mislabelled for the application, DPI allows a demon to see the contents of the packet and match it to the correct profile. This technology not only expands the scope of an algorithm's perspective, but DPI firms boast that their technologies facilitate new ways for network managers to comprehend their traffic.

Firms selling DPI appliances have grown considerably since their origins in network firewalls and IP switches. Bendrath and Mueller suggests six factors driving the industry: network security, bandwidth management, government surveillance, content regulation, copyright enforcement and injection of advertisements into Internet traffic (2011, p. 4). These factors seem to be at work publicly in the recent bills to filter copyright content on the Internet in the United Kingdom (Orlowski, 2011) and United States (Anderson, 2011; Masnick, 2011) or speculation a pending bill in Canada will grant police *lawful access* to ISP records (Chase, 2011; Geist, 2011c). Even these bills do not fully capture the forces driving the traffic

management industry since military and security experts also seek to deploy these appliances to create intelligent and secure networks (McConnell, 2011), no doubt to avoid hacks of government IT infrastructure (Woods, 2011) and the spread of worms (Zetter, 2011). Given the array of issues driving the industry, it should come as no surprise that Heavy Reading (2011), research consultants, predict the value of the industry will more than double in the next five years from $114 million in 2011 up to $357 million in 2016. Their recent report lists over 18 firms selling DPI products, up from 8 selected in a similar report from 2009 (Finnie, 2009).

Better perspective 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. However, DPI "is a black art in which both false positives and false negatives are unavoidable" (Finnie, 2009, p. 8); users often encrypt their packets to elude packet inspection. The industry responded with new methods to identify applications by the patterns in their packet flow. A Skype conversation sends packets at a different rate than browsing the web. Flow inspection allows demons to see the flow of a single user in addition to packets themselves. These two components augment the gaze of demons allowing them to identify the actual content of the packet even if it differs from the type specified by the port number or content (Finnie, 2009).

These two types of detection algorithms enable new policy management algorithms to better manage IP flows. 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, p. 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 use policy servers to apply DiffServ to slow its movement. Policy management demons, then, might be the most advanced form of QoS demons, capable of imagining highly complex, individuated networks for customers and applications.

Both DPI and DFI illustrate how QoS demons have a marked difference in expressing a living present during transmission. They have a greater ability to understand and profile a packet. This capacity links to policy servers capable of grouping kinds of traffic together into classes. Transmission shifts from Best Efforts model to the deliberate efforts of demons that mold the modulating times of the Internet into tiers and service levels. The capacities of QoS demons have resulted in a growing industry.

ISPs have begun to use QoS to manage the Internet's asynchronicity to override or enhance the decisions at the end. In doing so, they create a kind of *poly-chronous* temporal economy. It differs from asynchronicity in that it involves establishing tiers of temporalities on the Internet rather than allowing the ends to create as many possible. Poly-chronicity does not involve any attempt to reassert a synchronous communication rather it attempts to prune or management of temporalities. The economy involves asymmetrical relations where core network demons can override decisions of the ends and impose temporalities. A poly-chronous temporality remains in development as can be seen in the final discussion of the journey through the Pandemonium of the Internet.

From an Asynchronous to Poly-Chronous Pandemonium

The walls of Pandemonium stretch from each end of the Internet – often idealized as one home computer talking to another. In reality a bevy of networks route a packet from its source to its destination through fibre-optic lines, central offices and peering stations. A packet enters one end of the citadel and exits at the other end. During its stay, the packet encounters all sorts of demons who pass it along. Each encounter confronts the packet with demons who toil to route packets from various sources to different destinations. They act as a common path for all the packets traveling online. Often the journey is not with its conflict. Demons argue and debate amongst each other over a message and its future, the outcome of their debate determining the duration of the packet within the halls of Pandemonium. Demons, with their biases, desires and dreams, enlist packets as part of conspiracies between them.

Their perspectives and logics lead demons to form pacts and conspiracies that sediments into different actual networks or spires. Two grand spires loom over Pandemonium, Quality of Service (QoS) and End-to-End (E2E); however, fragmentation has occurred within E2E with a narrow version, a broad version and a peer-to-peer version emerging. Figure 10 depicts the four spires of Pandemonium. Horizontally, each segment depicts a different part of a packets journey from Sender to Receiver, across ISP networks, aggregation hubs and backbones. The vertical axis shows roughly the intelligence of the demons at each segment corresponding with the seven-layer OSI model. (The numbers are approximate and meant only for illustrative purposes.) The QoS network located demons almost as intelligent as the ends with ISP networks, where a P2P network only locates intelligence with its ends. These different spires compete against each other. A packet encourages a hybrid of these networks as demons

attempt to hijack a packet from one spire to another. This array of demons compose the nature of control within the assemblage of the Internet.

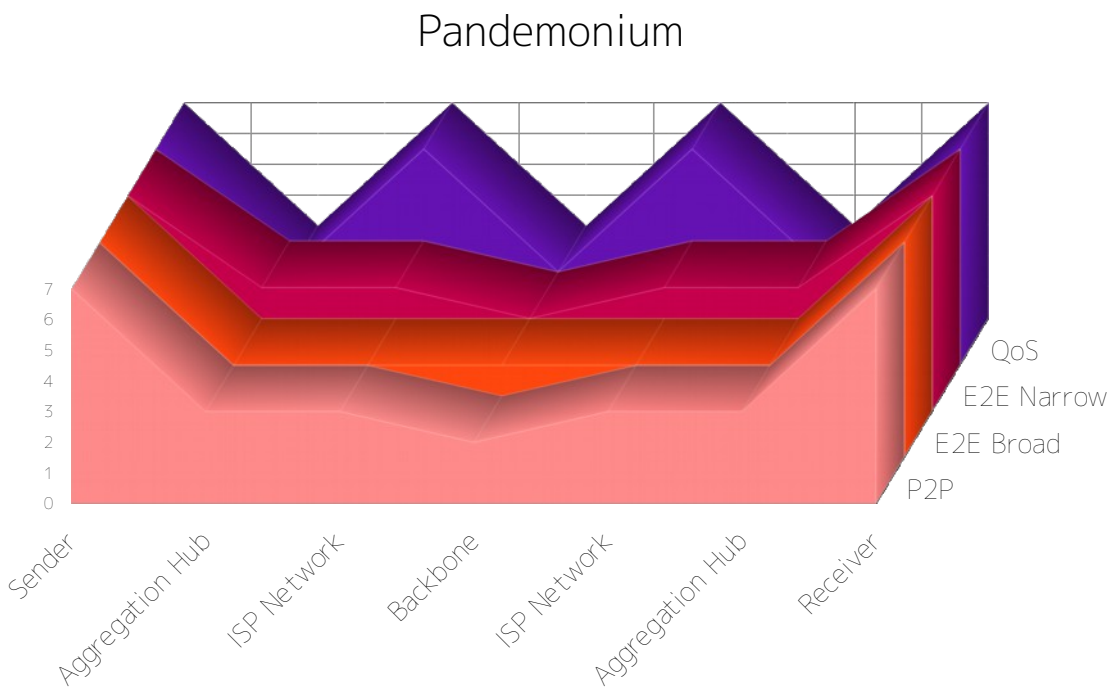


Figure 10: The Spires of Pandemonium.

The metaphor of Pandemonium also can b a guide through speculations about the daily operations of one of Canada's largest ISPs. Consider the schematics of the Bell's Digital Subscriber Line (DSL) network according to Bell's submission to the CRTC during the Review of Billing Practices for Wholesale Residential High-Speed Access Services seen in Figure 11 (Bell Canada, 2011). It outlines the passage of a packet and the demons it encounters. The passage beings with the Bell's home customer who launched an application attempting to communicate with another part of the Internet. In doing so, the application synchronizes two points of

the network. The work of demons at both the sender and the receiver send and recieve packets of information with a source, destination, a port to identify its type of application and many other control information. These demons assume they have ultimate control over the priority of the passage of the message. This power wanes as it passes from the computer's ethernet jack to a home router or modem connected to the Internet. Usually this device simply forwards the messages onwards, but concerns over home network security have introduced demons in this hardware as well. Often routers behave like simple firewalls or enact QoS decisions – for the most part these rules depend again on the user configuring their router and delegating certain repetitive decisions, such as properly transmitting BitTorrent traffic. The demon also converts the packet so it can be carried over Bell's telephone lines. As the packet moves outside the home, it slips outside the hands of end demons and into the frenzy of demons in the network outside.

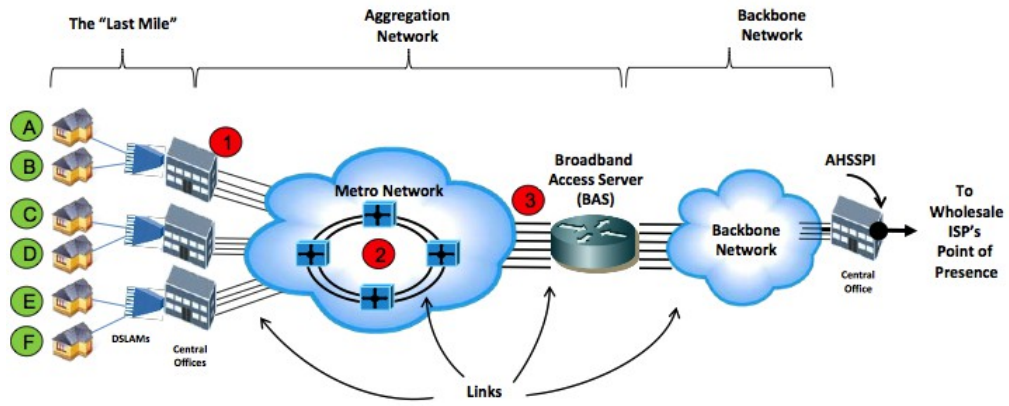


Figure 11: The Bell Network

The next stage of the journey involves Bell's own network. The first point, the Digital Subscriber Line Access Multiplexer (DSLAM), aggregates home traffic and passes it to Bell's aggregated backbone. Now a fog sets in as packets enter these networks; it cloaks the work of the demons at this point. A DSLAM would simply ferry the information deeper into the network; however, newer DSLAMs include some packet filtering, DiffServ and other QoS fea-

tures. These DSLAMs are marginal players since they commonly reside in a regional central office or even at a neighbourhood level. The true malevolent demons – mighty enough to content with the end demons – reside in the Broadband Access Servers (BAS) or Broadband Remote Access Server (BRAS, B-RAS or BBRAS). The demons at this point sulk about in deep fog – their movement only placed upon in technical documents or CRTC hearings (Canadian Radio-television and Telecommunications Commission, 2008, 2009a, 2009b).

Passing a packet to the Internet mirrors packet moving from an end to the core. The core sends packets to its host through major Internet backbones or other networks. BASs peer with other networks in major aggregation hubs or carrier hotels scattered across the world. Toronto, for example, has a major exchange point at 151 Front Street. These hubs allow networks to pass traffic between each other according to peering agreements[8] – many being confidential contracts that determine the rates and volume for traffic exchanged (McTaggart, 2006). The packet eventually leaves the core network either to a server delivering content or in the case of peer-to-peer to another computer on a residential network.

In this journey, the moment a packet enters an ISPs core network, they become subjects of QoS demons. Most Internet Service Providers in Canada and the United States use traffic management software to tier Internet transmission rates as seen by the ComCast case, thereby expressing a complex temporal economy. Bell Canada throttles peer-to-peer BitTorrent traffic during peak hours. Bell's networking code identifies BitTorrent packets or even patterns in packets equated to BitTorrent communication (Bell Canada, 2009a). Identified packets receive less bandwidth and, to the user, move slower on the network. Quality of Service algorithms not only slows P2P traffic. Rogers Communications argues peer-to-peer file

[8] These agreements constitute another forms of control and remain a significant point of debate over Internet control.

sharing is "the least effect 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). 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. In the 2009 CRTC's Internet Traffic Management Practices hearings, Bell stated their shaping "is based on managing traffic 'flows' and not individual content" (1994, p. 44). They continue that "DPI technology deployed by Bell Wireline has the ability to identify the source IP address and the destination IP address of both the sender and the receiver of the communications exchanges, when creating and managing flows" (2009a, p. 44). Bell, as has been widely discussed, throttles BitTorrent flow, but also, as it has alluded to, privilege certain subscribers traffic over others. While their attention may differ to the packets, their goal is to link sender and the receiver. A packet might simply turn back to another customer on the Bell network or pass on to the wider Internet.

These examples provide preliminary evidence that commercial Internet service providers have begun using demons and transmissive control to find new value in their networks by producing and assigning temporalities of transmission. Even though the Internet contains many demons, the intensification of traffic management software has bolstered the numbers of QoS demons on the Internet. Not only does Deep Packet Inspection allow for granular manage of flows, but QoS in general allows for a contraction of control back into the network in a move akin to broadcasting or telecommunications temporal economies. Certainly with most major ISPs coming from one of these two industries, these might be a desire to return to past temporal economies; however, their vision is not simply a repeat of past temporal economies.

This new *poly-chronous* temporal economy is a new kind of Pandemonium resembling the writings of Milton and Selfridge. Neither version of the capital contains disorder or chaos. Milton only introduces Pandemonium after Lucifer rises to command the other forsaken of Heaven who then construct a capital city where they might plan their revenge against the God that expelled them. Selfridge's Pandemonium was not chaotic, but ordered by the alphabet – a system of information in the thought of Deleuze and Guattari. Demons behave in a more systematic fashion to manage the input of shapes into output as machine-readable letters. Demons act according to the logic of an alphabet not chaotically. Alphabets – as the expressive part of a written language – function as a collective assemblage of enunciation. These analogies mimic the order of polychronous communication.

Where once the Internet literally could be seen as a Pandemonium of Internet routing demons with no central authority, it now has an order emerging from QoS algorithms. QoS demons has asymmetrical capacities to control transmission in spite of the dictates of an end. Both Milton and Selfridge offer a version of asymmetrical relations of transmission with asymmetrical authority. Lucifer or the decision demon had final say in their Pandemoniums just as QoS algorithms have final say over Internet routing. This breaks with the version of E2E where there was some symmetry in each node agreeing to a certain rare of transmission. Even though it might be easy to imagine QoS as the establishment of a centre or sovereign from the demons of the Internet, its more accurate to imagine their pact as a kind of alphabet that they agree to participate within. Their logics distribute throughout the Internet as denoted by the *pan* and their intelligence overshadows decisions made at the ends.

More and more, ISPs leverage their transmissive control to create a *poly-chronicity* to create a network optimality that reduces and manages the temporalities. It produces and assigns various temporalities that have comparative values. Multiple temporalities have a comparative

values to each other. It is akin to prime time television. Certain time slots have more value than others; however, the times of a tiered Internet have less to do with the hour of the day than the relations between times. File-sharing is assigned less priority. Its forces of coordination and exchange cease to operate optimally. In its place, a network imposes a centralized becoming of audiences receiving messages from fixed producers. Polychronicity is driven by a profound new ability to remake itself always in the name of network optimality. Network Neutrality is then only the beginning of the problems of poly-chronicity. As more ISPs leverage their expanded capacities of transmissive control, the temporalities of the Internet will change even more.

Conclusion

This chapter began by questioning the particular conditions of algorithms to function as means to control transmission. Their capacity depends on digital information and digital programming. The two allow for the Internet to enact an *asynchronous communication* that modulates for different applications and types of communication. Digital programming and digital information manifest within algorithms as profiling and logics. Algorithms monitor packets and compare their bits to patterns embedded in their memory. This process converts the variable packets into inputs for algorithms logics to manage and shape. Every bit that travels before a packet triggers this process. The moment of routing then becomes a living present in the words of Deleuze that realizes a variable transmission of information. Transmissive control occurs in this moment of profiling and logics. Their interoperation produces and assigns a temporality for each packet.

Demons were the metaphor for this chapter to explore the various algorithms of the Internet. These demons conspire in the depths of Pandemonium to route packets according to cer-

tain visions of networks. Two kinds of demons appeared in this investigation. Broad and narrow E2E demons tend to be simpler algorithms that leave complicated routing decisions to the ends of the network. Quality of Service demons, on the other hand, have begun to leverage on their intelligence to assert the rights of the network to control information. These demons conflict and chaff, but recent advancements in traffic management software have advanced the power and influence of QoS demons. These demons have begun to express a poly-chronicity online defined by tiering and stratifying temporalities.

Transmissive control may be better understood through these demons. The production and assignment of temporalities depends on certain demons with modulating capacities of transmission. Demonic traits – programming and perspective – create patterns in the transmission of the Internet. These patterns form to become its temporality. Many temporalities existed during the dominion of end-to-end transmission. Their symmetrical relations allowed for two ends to agree to new forms of transmission. Asynchronicity had a value to many in being open enough to allow for innovation. This form of transmissive control, however, also proved too open as worms, congestion and the need to guarantee rates for important communication led developers to seek new ways to control Internet transmission. Quality of Service algorithms mark a major change in the nature of transmissive control on the Internet. They allow the Internet to be at once full of multiple temporalities, but to create stratifications and tiers among these temporalities. Quality of Service promises to turn the Internet into a polychronous communication system with a complex temporality of valuing one temporality over another.

Poly-chronicity, however, has not completely crystallized. This chapter has developed a tension in the Internet between advanced traffic management software as seen in Quality of Service algorithms and end-to-end algorithms. E2E demons continue to undermine the crys-

tallization of the poly-chronicity. Nowhere is this more evident than in the case of The Pirate Bay and its attempts to undermine transmissive control. The next chapter then moves to a consideration of how advanced traffic management attempts to capture piracy and how The Pirate Bay attempts to elude capture. It is a story of the hunt and escape that illustrate the competing trajectories of the Internet of poly-chronicity and its enemies. This chapter studies these trajectories through experimenting with an actual appliance to show how it profiles and it applies certain networking logics. This hunt drives the Internet onward into its own becoming.

The shift in topic again requires a shift in metaphor. Where demons help understand the otherness of transmissive control and *Inception* helps explain asynchronicity, the novel *Moby-Dick* helps explain the nature of control and its limits. Both novel and chapter involve a hunt that transforms the hunter. Transmissive control hunts piracy, where Captain Ahab, a central figure in the novel, hunts for a White Whale. Where Ahab is driven mad, transmissive control is driven to advance to even greater length of managing transmission. These directions resemble the lines that Deleuze and Guattari assign to the assemblage mentioned in Chapter One. The metaphor of *Moby-Dick* helps characterize these lines. When Deleuze spoke of these lines, he often refereed to the work of Herman Melville and *Moby-Dick*. He would describe the White Whale as a line of flight, the madness of Ahab as a line of becoming and the order of his ship as a series of rigid lines. The Pirate Bay produces lines of flight to elude the operations of transmissive control. At the same time, transmissive control tries to draw its own stable lines into the future of the Internet. These tensions – found in both the novel and this chapter – between control and its limits help characterize the becoming of the Internet.

Chapter Four: The Hunt

Introduction

All visible objects, man, are but as pasteboard masks. But in each event- in the living act, the undoubted deed- there, some unknown but still reasoning thing puts forth the mouldings of its features from behind the unreasoning mask. If man will strike, strike though the mask! How can the prisoner reach outside except by thrusting through the wall? To me, the white whale is that wall, shoved near to me. Sometimes I think there's naught beyond. But 'tis enough. He tasks me; he heaps me; I see in him outrageous strength, with an inscrutable malice sinewing it. That inscrutable thing is chiefly what I hate; and be the white whale agent or be the white whale principal, I will wreak that hate upon him. - Captain Ahab

The last chapter ended with a conflict emerging between a transmissive control expressing a poly-chronicity and the older E2E algorithms that still operate asynchronously. It would be misleading to assume that Quality of Service transmissive control will have an easy victory in its crystallization of a poly-chronous Internet. P2P hackers and pirates continue to taunt and gnaw at the limits of transmissive control. They attempt to create "vacuoles of noncommunication" that elude transmissive control (Deleuze, 1995a, p. 175). This chapter focuses on how pirates to expose the limits of transmissive control. It explores the limits of transmissive control. As Beniger states, "control of any purposive influence can be no better than its most generalized and distributed processor of information" (1986, p. 391). Transmissive control, as the quote suggests, is no better than its ability to capture and respond to the exposure of its limits. This chapter uses a new metaphor to aid in its discussion of the limits of transmissive control.

A captain, a ship and crew seems to describe the system of order and control. Only through a precise system of control, as Laurie Anderson points out[9], does the ship succeed in

[9] Her discussion of *Moby-Dick* comes from her work *Songs & Stories of Moby-Dick* featured in a Studio360 podcast. The episode is accessible here: http://www.studio360.org/2011/dec/30/.

its hunt for whales. Herman Melville describes such an assemblage in his novel *Moby-Dick*. Its whaling ship, the *Pequod*, appears to offer this metaphor for control as it leaves port from Nantucket. Orders from its Captain and tensions in the ropes of the ship function as forms of control that allow the ship-assemblage to navigate the oceans of the world; but this metaphor of control evaporates as Ahab utters the quote above. Beneath the discipline he imposes on the crew, an unfathomable fury drove him to tirelessly hunt for whales. Through this quest, Ahab seeks to look beyond the "pasteboards masks" of the world into the "unreasoning" limits of his control and this limit is Moby-Dick, the white whale that parted him from his leg. His quest forms the plot of the novel. Ahab characterizes the hunt of control to forever attempt to capture its limit. He is monomaniacal in his desire to kill Moby-Dick.

The hunt for pirates resembles Ahab's hunt for the White Whale. Moby-Dick avoids Ahab's harpoons by running away or diving away. These tactics buy it time to live, to survive. A similar leviathan lurks in the depths of the Internet enraging copyright holders and network administrators. The Pirate Bay (TPB) are a group of Swedish hackers and anti-copyright activists that claims to be "world's most resilient BitTorrent site", among other tactics. The bond between the whale and Ahab, which seethes in Melville's book, also resonates with The Pirate Bays's own tumultuous history with the copyright industry and network administrators. Just as Moby-Dick embodies the limits of Ahab's mind, The Pirate Bay charts the limits of transmissive control. From their humble start in 2003, The Pirate Bay pushed back against deployments of control on the Internet – from the attempts to remove illegal content from the web to the more recent attempts to filter and shape modes of communication.

The Pirate Bay is a paradigmatic case in the study of peer-to-peer networks and piracy as antagonists to the emerging poly-chronicity of the Internet. The Pirate Bay has been the world's best known BitTorrent search engine and tracker. Despite much legal pressures, as

will be discussed, it kept its site open and, in doing so, pushed piracy into every greater levels of publicity. They have fought for a future Internet that resists a poly-chronicity. Without The Pirate Bay, BitTorrent perhaps would have neither consumed the share of global bandwidth as it did nor would piracy be a political movement sweeping Europe. Though many other pirates operate online, The Pirate Bay is the biggest and fiercest of pirates clogging profitable networks with its peer-to-peer transmissions. This struggle – of networks trying to eradicate The Pirate Bay and of The Pirate Bay trying to continue – charts the limits of transmissive control.

This chapter describes two of their attempts to delay capture by control: its BitTorrent tracker website and its virtual private network service iPredator. Each offers a new twist and tactic away from transmissive control. As the terror of P2P networks became apparent to the copyright industries, they sought out to destroy these networks. Legal victories crippled the first generations of P2P networks and soon a legal trial ensnared The Pirate Bay. As their site continued in spite of these legal hunts, a new threat loomed. Traffic management algorithms offer ISPs a means to alter the nature of transmission on the Internet to control the very channels of transmission. In response to the growing usage of traffic shaping, The Pirate Bay changes strategies. This chapter explores this move through a discussion of iPredator. It explains how iPredator works and describes the hunt for BitTorrent and iPredator by the PacketShaper. It provides a thick description of how one exemplary piece of software – the Packeteer PacketShaper 8500 – detects BitTorrent and iPredator traffic.

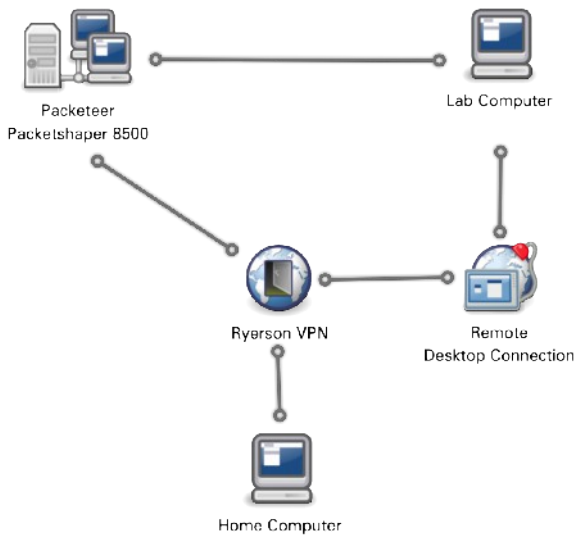


Figure 12: The Test Lab

A test lab helps to render capture and elusion. The test lab, as depicted in Figure 12, connected a stock Windows 7 labeled 'Lab Computer' connected to the PacketShaper 8500 and out to the Internet. It directly links to a PacketShaper 8500 in effect controlling for the irregularities in traffic. Only communications originating or terminating with the Lab Computer would be inspected by the PacketShaper. By logging into the Ryerson VPN, testing could manipulate both the PacketShaper and the Lab Computer. The test lab offers a chance to understand the potential of traffic management software and the activity of The Pirate Bay.

Understanding the struggle between The Pirate Bay and transmissive control helps explain the becoming of the Internet. Just as the White Whale drives Ahab onward, piracy spurs innovations transmissive control. Piracy is a central driver in the development of transmissive control as it threatens networks with insecurity and congestion. It exposes the limits of control, but also provides a reason for transmissive control to improve. This dynamic contributes to the larger dissertation by showing how transmissive control adapts to its limits.

This chapter concludes with reflecting on this unintended consequence of piracy, namely coaxing transmissive control to become even more intense.

Transmissive Struggle: Drawing the Lines of Elusion

Understanding the relationship between piracy and transmissive control requires a more complex discussion of the becoming or trans-individuation of networks. This becoming is understood in the work of Deleuze through the concept of lines. They inhabit all his writings particularly his writings on *Moby-Dick*. He describes Ahab and his madness as a becoming something else, "turning into a line of abolition, annihilation, self-destruction, Ahab" [italics added] (Deleuze & Guattari, 1987, p. 250). His journey is another line, as the harpoon and the whale are a line too. These many lines in the language of Deleuze and Guattari compose the novel *Moby-Dick* just as they conceptualize their own writings. Lines will also explain the trajectory of the Internet.

Central to the study of an assemblage, like a book or the Internet then are lines. If ropes, nautically called lines, form a complex rigging of tensions and speeds to pilot a sailing ship, then lines in the work of Deleuze and Guattari are akin to the rigging of an assemblage. Literally, they bind an assemblage together, as in the case of the harpoon in the whale. "Thinking in terms of moving lines was Herman Melville's operation: fishing lines, diving lines and dangerous, even deadly, lines" (Deleuze, 2007a, p. 343). Through a system of lines, a ship acts as an assemblage with certain lines manifesting functions and characteristics of the boat, such as raising or lowering the sails, to create an assemblage of conduct and circulation. Lines provide the theoretical concept to explore the struggle on the Internet and its becoming that results from the struggle to control transmission and to elude control.

Deleuze offers three kinds of lines to understand a collective becoming. He offers three terms again through the example of *Moby-Dick*. "Nothing is more complicated than the line or the lines", as Deleuze writes, "it is that which Melville speaks of, uniting the boats in their organized segmentarity, Captain Ahab in his animal and molecular-becoming, the white whale in its crazy flight" (2007b, p. 103). These three lines inhabit the world of Melville and the mind of Deleuze as he explores the *segments*, *cracks* and *ruptures*. Consider the lines of *Moby-Dick* as a way to explain the types of lines. The first type refers to the ordered lines of the ship. These lines code the operations of the ship and participate with a second line to create an order. Even though the whaleboat might have an order, Ahab has broken with the code of whalers in the quest for a white whale, "in a choosing that exceeds him and comes from elsewhere and in so doing breaks with the laws of the whalers according to which one should first purse the pack" (Deleuze & Guattari, 1987, p. 244). Ahab becomes something else, though oddly bound to the white leviathan whose otherness continually flees from his understanding. The third line being the flight of the whale. These three lines – a line of flight, a supple flow and a rigid line – are a part of the composition of communication and information. Lines and the study of lines offer a framework to engage the hunt and elusion of transmissive control.

As an order bellowed from the Captain travels across the deck of the boat, it imposes an order on the crew. The discipline of the Captain unites the ship, it functions as a line of *rigid segmentarity*. His orders compose the crew into segments with specific functions and expectations. The packet involves the segments of the line. Deleuze states, "segments imply devices of power" (2007b, p. 96) and,

> Segmentarity is inherent to all the strata composing us. Dwelling, getting around, working, playing: life is spatially and socially segmented. The house is segmented

> around its rooms' assigned purposes; streets according to the order of the city; the factory according to the nature of the work and operations performed in it. (Deleuze & Guattari, 1987, p. 208)

Segmentarity is a general concept as capable in the seas of Melville as in routes of the Information Superhighway. Transmission as packets, with their headers and average bit rates, is another segmented line. Encoding a message as packets cuts (a word that Deleuze borrows from F. Scott Fitzgerald) to discuss the rigid break in a line (2007b, p. 94). Rigid lines code a message into discrete units of information. These segments create rigid lines or, in other words, packets create flows that can be read and managed by traffic shaping software. The grid stretches out, turning binary signals into a plane of control.

With these rigid lines, the steersmen at the helm charts a course, setting the ship on a journey and becoming. This course expresses another line and a second kind of segmentarity. An understanding of this line corresponds with a sense of the madness of Ahab. Consider the passage of Deleuze on the crazed quest of Ahab,

> What is Ahab doing when he lets loose his harpoons of fire and madness? He is breaking a pact. He is betraying the Whalers' Law, which says that any healthy whale encountered must be hunted, without choosing one over another. But Ahab, thrown into his indiscernible becoming, makes a choice – he pursues his identification with Moby-Dick, putting his crew in mortal danger. This is the monstrous preference that Lieutenant Starbuck bitterly objects to, to the point where he even dreamed of killing the treacherous captain. (Deleuze, 1998b, p. 79)

What does Deleuze mean when he speaks of Ahab breaking the Whalers' law? What is Ahab doing when he makes his fatal choice to pursue the white whale? His choice shifts the very ground – the planks of the deck so to speak – where his crew stand. The rigid segments of the

whaling ship demand a code of conduct toward whales and underlying every knot and crank is a sense of that order. Not only does it bind sailors, but its financiers who expect a cargo of oil and ambergris when the ship returns to Nantucket. This law is a *supple line* woven into the actions of its crews and its rigid lines. As Deleuze and Guattari write, "it is not sufficient to define a bureaucracy by a rigid segmentarity with compartmentalization of contiguous offices...there is a bureaucratic segmentation, a suppleness of and communication between offices" (1987, p. 214). Along with the rigid lines that create the office space or the roles of the sailors that create an order-able crew, the supple lines takes the helm. The supple line imposes an order that repeats upon the crew, supplying a predictability and a future, in part due to is suppleness. What Ahab does, in his own quest, is to create a new supple line on its becoming. His madness never erodes the discipline of his whalers on their death-ship, but it does lead them far off their traditional course.

The supple line involves the abstract processes of networking immanent within the operations of control. Software pulls the lines together or push away from its other. The line depends on protocols to translate the communication into its segments; however, flows contain the line. The line – the packet – does not fully enclose the flow and the line overflows. Packet by packet, flow by flow, traffic management software expresses the supple line. Packets on their own lack an overall order; they are the units of a becoming-network. This becoming is not simply spatial as a network form (see McKelvey, 2010); rather, as Parikka suggests that networks have a *temporal becoming* that are "multiscalar and the affects of network culture involve not only technology, but also a whole media ecology of politics, economics and, for example, artistic creation" (2010, p. 55). A supple line, then, refers to the unfolding temporalities and relations of temporalities of a network, usually to impose a degree of regularity to the bursts of packets.

As transmissive control shapes packets, it expresses a collective assemblage of enunciation and this process is a network-becoming. It allows for an asychronicity or polychronicity.The result, similar to the State Apparatus, seeks to regularize the temporality of the Internet. For Deleuze and Guattari, the State Apparatus "never ceases to decompose, recompose and transform movement, to regulate speed" (1987, p. 386). Segmented lines offers a way to regulate movement as it turns communication into "a place of organization" (Deleuze, 2007b, p. 102). Sedentary roads, as introduced in the quote at the beginning of this chapter, exemplify the product of a State Apparatus. It enlists segmented lines and supple flows to produce a regularity or systematic relationship between speeds. Difference, to remember the early Deleuze (1994), becomes repetition. Information travels on trodden paths or to remember the nautical theme, through charted waters and known seas.

The supple lines also conceptualizes the becoming of a poly-chronous Internet. Segmented lines of packets manifest temporal economies within the dominion of transmissive control. Their constant efforts create regularities of communication indicative of networks. Algorithms function at a material level to transmit packets and also at an abstract level to actualize a temporal economy. To recall the discussion of communication and information from the Introduction, the regulation of speed is the expression of a communication system that effects the distribution of information. How information circulates defines the collective assemblage of enunciation and the becoming of a network. Repetition produces predictable networks with a promise of a known future that continues the rates of transmission found in the present. Yet, an assemblage that regularizes temporalities only appears novel in contrast to its outside, to irregularity. It is a complete becoming due to the efforts of piracy. Supple lines attempt to capture and control the transmission of packets and to bring any deviations back under control. This outside speaks to a third line at work on the Internet.

Deleuze and Guattari also speak of a final line, a nomadic one that continually flees and melts away. This is the line of the flight and it runs through the course of this chapter as Moby-Dick haunts the mind of Ahab throughout the voyage of the *Pequod*. The line of flight refers to something "even more strange: as if something carried us away, across our segments, but also across our thresholds, toward a destination which is unknown, not foreseeable, not pre-existent" (Deleuze, 2007b, p. 104). If the purpose of the collective assemblage is to normalize, then the line of flight seeks to experiment. They are the bane of mechanisms of control and capture. Lines of flight pull transmissions from its representation by the packet and from the capacities of transmissive control. The Pirate Bay is the chief source of lines of flight in this chapter. After an introduction to the group, this chapter moves to explore the lines generated by them.

The Pirate Bay and the Line of Flights

The Pirate Bay began as a project of the Swedish Piratbyrån that ran from 2003 until 2010 after the death of co-founder Ibi Kopimi Botani (Ernesto, 2010a; Norton, 2006). It "was initiated to support the free copying of culture," stated two of other vocal members of the organization, Rasmus Fleischer and Palle Torsson (2007), "and has today evolved into a think-tank, running a community and an information site in Swedish with news, forums, articles, guides and a shop and has to date over 60,000 members" (np). Even its name, Piracy Bureau in English, exemplifies the advocacy and humorous tone of the group mocked the Svenska Antipiratbyrån or Swedish Anti-Piracy Bureau Members of group described it as "a cluster with fuzzy borders, a network consisting of a number of connected humans and machines; artists, hackers, activists, servers, routers and software, each approaching the question of copyright in its own manner" (Eriksson, 2006, np.). The best-known achievement of the group was the

launch of a BitTorrent tracker and search engine called The Pirate Bay in 2003. As Rasmus Fleischer, co-founder of Piratbyrån recalled, "it started off as just a little part of the site. Our forum was more important. Even the links were more important than the [torrent] tracker" (Daly, 2007, np.).

Figure 13: Picture taken of The Pirate Bay in 2004.

At the time of launch, the site was just one of the services the Piratbyrån provided and not necessarily the most popular. At the time it ran on a Celeron 1.3GHz machine with 256MB RAM seen in Figure 13 that shows the servers running The Pirate Bay[10]. It first ran on the black laptop, but by this time had expanded to three servers (Ernesto, 2011b).

The site became so popular, the Piratbyrån decided to split the site into a separate organization. They gave control to three members of the bureau: Gottfrid Svartholm (aka: Anakata),

[10] The images comes from The Pirate Bay's own image gallery of servers present and past that can be found here: http://static.thepiratebay.se/tpb/.

Fredrik Neij (aka: TiAMO) and Peter Sunde (aka: brokep). All the members of the site are male and in their twenties. As Gottfrid Svartholm states, "I see The Pirate Bay as a sort of organized civil disobedience to force the change of current copyright laws and the copyright climate" (Kurs, 2007, np.). These three administrators work in their spare time to run the site and also publicly represent the site. Mikael Viborg, a prominent lawyer in Sweden, also provides the site with legal assistance (Norton, 2006). The site also relied on volunteers and moderators. Although the two groups shared no legal connections, they acted as a united front against copyright with the Piratbyrån acting as a think tank and TPB enabling users to share files.

The Pirate Bay sought to create times of piracy on the web by disrupting the operations of transmissive control. Its line of flight disrupt the rigid lines, further driving a gap between it and the supple line to allow moments of piratical transmission. In this way, transmissive control makes the same, where The Pirate Bay does the opposite. It disrupts these retentions and repetitions. Deleuze and Guattari would call The Pirate Bay a nomadic war machine. A nomadic trajectory, they explain:

> does not fulfill the function of the sedentary road, which is to parcel out a closed space to people, assigns each person a share and regulating the communication between shares. The nomadic trajectory does the opposite: it distributes people (or animals) in an open space, one that is indefinite and noncommunicating. (1987, p. 380)

Temporal economies follow a sedentary road or a set path and in doing so, establishes collective assemblages of enunciation. The nomadic path may be said to create non-communications in that ruptures paths and creates discontinuities. These moments allow for the proliferation of piratical modes of communication. This nomadic path is a vital component of the becom-

ing of the Internet. In following the nomadic path, The Pirate Bay traces out the possibilities of transmission and the limits of online control.

The Pirate Bay has continually produced new lines of flight to thwart the operations of transmissive control. As a nomadic war machine, they engage in a nomadic science (as opposed to the State's royal science) that see new weapons and trajectories to elude transmissive control. Its science involves many forms beyond just a kind of escape. Vacuoles, glitches and hacks, the war machine will use all available weapons in its fight to elude control. Deleuze and Guattari position the war machine as an ulterior becoming against the Royal becoming of the State Apparatus. This is not to confuse ISPs owners with the State (although one could argue the point), but to suggest that the development of traffic management algorithms to normalize traffic fits within a kind of official mode of production. The Pirate Bay, on the other had, offers an alternative form of production of P2P networks. As Deleuze and Guattari write,

> On the side of the nomadic assemblage and war machines, it is a kind of rhizome, with its gaps, detours, subterranean passages, stems, openings, traits, holes, etc. On the other side, the sedentary assemblages and State apparatuses effect a capture of the phylum, put the traits of expression into a form or a code, make the holes resonate together, plug the lines of flights, subordinate the technological operation to the work model, impose upon the connections a whole regime of arbolescent conjunctions. (1987, p. 415)

Where the State Apparatus seeks to produce a hierarchical tree of predicable futures or, the sedentary assemblage, the nomadic war machines is rhizomatic in its capacity to become something new at any point. The Pirate Bay, then, is an innovator, continually developing new holes and detours. Lines of flight involve a strategic dimension to their trajectory.

Many examples illustrate the different lines The Pirate Bay (TPB) develops to threaten network owners. Their Legal Threats page frequently responded to takedown requests by media firms and holders of copyright with sly, offensive and rude remarks. TPB has also symbolically brought back a shutdown tracker as a sign of the resilience of file-sharing. To date, TPB has circulated confidential documents leaked by Anonymous and LulzSec as well as mirrored documents from Wikileaks including the so-called Insurance File that contains all leaks in one encrypted file that Julian Assange threatens to release if provoked[11]. The popularity of the site also played an important role in the genesis of the pro-piracy movement in Sweden. As Miegel and Olsson writes,

> the Pirate movement represents a new generation of voters and politicians, claiming to reform the classic political and democratic agenda and its issues and values by adapting them to a society built on a new technology and around individual lifestyles tied to the actual use of the technologies' potentials. (2008, p. 215)

The Piracy movement led to the rise of a Political Party in Sweden that attracted 0.65% of the popular vote in the 2010 election. The movement has spread globally by winning seats in the European Union and Germany, as well as starting parties in most Western democracies (Li, 2009; Lindgren & Linde, 2012; Miegel & Olsson, 2008). These examples indicate the many different tactics used by The Pirate Bay, but this chapter in particular seeks to elaborate the two lines directly related to the limits of transmissive control.

Amidst all this activity, The Pirate Bay offers two critical lines of flight to elude transmission control: acceleration and escalation. These two terms first introduced by Rasmus Fleischer (2010), scholar and member of the Pirate-Bay-Affiliated Piratbyrån, offers a way to con-

[11] A few of the files mentioned might be found here: http://thepiratebay.org/torrent/5728614/Wikileaks_insurance_file, http://thepiratebay.org/torrent/6156166/HBGary_leaked_emails, and http://thepiratebay.org/torrent/6533009.

ceptualize a trajectory for transmissive control. Acceleration refers to eluding control by outpacing the mechanisms of capture where escalationism refers to the ability to hide or avoid detect from active forms of control. The first section of this chapter provides a history of the rise of the P2P networks, the rise of The Pirate Bay and the strategy of accelerationism – a term put forward by Fleischer – to describe the rapid expansion of peer-to-peer networks. The following sections explores this line of flight of accelerationism before moving to a discussion of escalationism.

Accelerationism and BitTorrent

Nevertheless the boats pursued and Stubb's was foremost. By great exertion Tashtego at last succeeded in planting one iron but the stricken whale without at all sounding still continued his horizontal flight with added fleetness. Such unintermitted strainings upon the planted iron must sooner or later inevitably extract it. It became imperative to lance the flying whale or be content to lose him. But to haul the boat up to his flank was impossible he swam so fast and furious. What then remained?

Whales, upon noticing their hunters, flee for their lives. The older whales often drawing the vessel away from their youth, hoping they might survive. They leviathans ran away across the expansiveness of the sea, often expending their twilight vitality. Pirates respond in the same way when realizing the hunt is on; they flee. Running away is one line of flight employed by TPB. Rasmus Fleischer describes this strategy of one of accelerationism. It, as he writes, meant "accelerating digital communications and enabling access" and the tactics were "fresh strategies which produced a kind of politics which did not fit into the Swedish party system" (2010, np.). Accelerationism believed in the open waters of the Internet – filled with hidden coves and seas to escape the hunt. Accelerationism, in other words, meant a continual pushing the limits of file-sharing, expanding into the unknown. Successive version of software – Napster, Gnutella, MojoNation and BitTorrent – intensifies a flight away from transmissive control. As fast as lawsuits killed P2P networks, new beasts joined the pack. Generations of

P2P networks developed in only a few years. The evolution of these networks demonstrates the acceleration strategy and the flight from the centre. The strategy of acceleration drove the proliferation of peer-to-peer applications and The Pirate Bay.

The Pirate Bay became and to some degree continues to be, the largest, most public BitTorrent search engine and tracker on the Internet despite constant legal threats. BitTorrent needs to be explained in relation to two predecessors, Gnutella and MojoNation. Innovations in their algorithms made their way into BitTorrent. Its worth discussing these two technologies in depth to explain how BitTorrent exemplifies accelerationism and how the success of TPB fuelled the growth of BitTorrent networks.

Gnutella accelerated the decentralization of the network past Napster by removing the need for a single tracking server as compared to Napster that required all users to connect to a common tracking server. Indeed, most of the early P2P clients kept a centralized network (Leyshon, 2003). When the server went down, the P2P network failed. Kan, developer of Gnutella, states that it "started the decentralized peer-to-peer revolution," prior systems, like Napster, "were centralized and boring" (2001, p. 121). No node on Gnutella was essential for the network because nodes not only shared files, but they also shared searches ensuring that no central index existed. Searches cascaded across nodes, eventually returning a query of thousands of nodes that might host a specified file. Secondly, Gnutella also decentralized the institution facilitating the network. Where Napster was a software application, Gnutella was a protocol: a standard for transmitting information online. Any software application abiding by the Gnutella protocol could access the network. Further, Gnutella was an open source project without any ties to a company. Open sourcing separated the content of the Gnutella network from the development of the software running the network. Where an instance of Gnutella could be shut down, the actual software had no connection to the content.

Although an innovative solution, another group of P2P hackers argued that Gnutella did not solve a key problem for P2P networks: uneven sharing and free riding. Jim McCoy of Autonomous Zone Industries argued that many users opted not to participate in the P2P networks, preferring to take and not give back. Free riding, the term to describe failures to participate, plagued Gnutella (Adar & Huberman, 2000). It not only degraded the flow of information on the network, but also threatened to replicate the early problems of centralization with Napster (McCoy, 2001). Again, hackers again saw a technical solution to the social problem. McCoy proposed the solution in his MojoNation product[12]. Autonomous Zone Industries launched their MojoNation in 2000 at DefCon, a famed hacker conference (McCullagh, 2000) where they explained how to eliminate the free rider problem and increase the resources of a P2P network. The answer, in short, re-thought transmission aways from a sender and receiver model towards a community of peers sharing their resources amongst each other. MojoNation broke a file down into pieces that it distributed across the network as a way to avoid censorship. Breaking the file down meant that no one node contained a whole file. In doing so, the system avoided concentrating files in any one server. Importantly, MojoNation was not a gift economy; rather, it attempted to create any economy of sharing by rewarding people when they shared files. Network software tracked how much a user shared. The more a user shared, the more capital or Mojo, they accumulated. Mojo corresponded to the amount of bits shared by a user not the amount of files. Users, in turn, exchanged their Mojo for space to upload their data, an early version of cloud computing. Autonomous Zone Industries hoped

[12] Though fuelled by venture capital, MojoNation oozed early computer piracy lore. The Autonomous Zone referenced Hakim Bay's anarchist manifesto linking data pirates to 18th century pirate utopia. The developers called themselves as 'Evil Geniuses for a Better Tomorrow' – a reference to a game by Steve Jackson Games (Cave, 2000). Fourteen years earlier, the police raided Steve Jackson Games after suspecting their new game Hacker to be a covert illegal operation. The raid triggered a wave of online activism that culminated in the launch of the Electronic Frontier Foundation, a leading advocate for digital rights (Sterling, 1992).

to capitalize off the amount of Mojo by charging a small transaction fee. Mojo, importantly, created a temporal economy of peer resource sharing, similar to a time-sharing system, yet, different because networked computers pooled their home-computer resources to generate more shared capacity. Further, the networking logic pushed away from any sense of sender and receiver since peers continually uploaded and downloaded files (Cave, 2000; McCoy, 2001).

Unfortunately, the innovations of MojoNation did not translate into financial success. Even though MojoNation collapsed, its innovations lead directly to BitTorrent. BitTorrent began as the personal project of an ex-employee of MojoNation, Bram Cohen. He quit his job at Autonomous Zone Industry and used his savings to work fulltime on fixing the problems he saw in its network code. Over the course of 2001, Cohen developed a new approach to file sharing that built on the insights of its predecessors. Following Gnutella, he chose to release an open standard, as well as, actual software. He released the BitTorrent protocol and client on 2 July 2001 to the forum: "decentralization · Implications of the end-to-end principle" (Cohen, 2001, np.). He had been testing the program for a few months prior (C. Thompson, 2005). The protocol built on the decentralization of Gnutella by removing the need for any central servers (though it did depend on decentralized trackers as will be discussed) and it enforced a temporal economy of sharing like MojoNation. The mixture proved explosive as BitTorrent consumed nearly half of all traffic until only recently with the rise of NetFlix (Sandvine Inc., 2010, 2011).

BitTorrent differs from other P2P applications by decentralizing the very network itself. Where Gnutella and MojoNation both attempted to create singular P2P networks, BitTorrent proliferates networks. In fact every file shared through BitTorrent has its own network of peers. It does so by inverting the logic of connection – where peers once logged into networks

to share files, Torrent files bring peers together into files. The Torrent file is the index that contains the meta-data necessary to participate in a BitTorrent network – it is the eyes of the demon to remember the language of the prior chapter. Appendix 4.1 lists all the components of a torrent file. The primary function of the torrent file is to provide an index of data being shared. Similar to MojoNation, BitTorrent approaches data as the sum of smaller pieces of information. The metadata lists the number of pieces and their sizes that comprise a file. Through reading the metadata and performing error checking on the pieces received, a BitTorrent client gradually assembles a complete copy of file. The metadata locates pieces of the file to the client. Beyond an index of data, the Torrent files also include instructions a client how to connect to a network. These instructions typically told a client to connect to a BitTorrent tracker: a website that keeps track of users sharing a Torrent file. Recent versions of BitTorrent have abolished trackers all together in favour of an even more decentralized approach, known as a distributed hash table, that store peers and locations dynamically within the swarm of peers sharing a torrent (Cohen, 2008).

The logic of accelerationism is embedded in the software of BitTorrent. Once a user has a file, their client connects to swarms of users who bits of the data indexed by the Torrent file. Peers share pieces of the data according to rules established in the BitTorrent protocol; the most important of these rules specifies a certain logic of sharing. A BitTorrent client enters a swarm by announcing its presence to the tracker that, in turn, announces the new client to the swarm. Peers understand new users according to two variables: choked and not interested. Choked means that the swarm will not send bits to the peer and not interested means the peer has elected not to request bits. These variables ensure every node that download also uploads. The golden rule of BitTorrent then is to force nodes to share their pieces. The more one shares, the more nodes will share other pieces, leading to a shorter download time. If a

peer does not share, it will be choked. In this way, every BitTorrent programs imagines and seeks to create a network where all nodes contribute data to the network. A new peer does not have anything to share, so it starts off choked. A peer finally receives a piece of the torrent through a function of the program known as *optimistic unchoking* where a node sends a peer pieces even if they have been classified as choked. New peers are three times more likely to benefit from optimistic unchoking than other peers. Typically, nodes will attempt to share the rarest piece of a torrent index based on a count kept by the tracker. Once a node has pieces and starts sharing them, other peers recognize it is sharing and unchokes the connection to send it more files. Peers know when to exchange files by disclosing what pieces they have and what pieces would like to receive. Through a constant exchange of TCP data packets and UDP control packets, a swarm gradually channels data to its nodes to ensure each receives a complete copy of the data being shared (Legout, Urvoy-Keller, & Michiardi, 2005). No uploader or downloader exists; rather, a BitTorrent peer simultaneously gives and receives data as part of the swarm. Continual exchange between peers ensure multiple copies of a piece exists in the swarm, ensuring the times of concentration MojoNation worried about without the complex centralized system of Mojo. Its strategy attempts to decentralize the network thereby growing it as fast as possible

While the BitTorrent protocol decentralizes P2P networking, it does require some central index of Torrent swarms and, in the past, a tracker to coordinate sharing. A number of website arrived to fill this void. Usually they took the form of a search engine. Sites like these index torrents found on the web or uploaded to their servers, a practice that varies from site to site. Once indexed, sites deliver torrents based on search results or based on an assigned category. Access also varies: public torrent search engines allow anyone to search, upload and download, where, increasingly popular, private sites require users usually to obtain an invita-

tion and maintain a positive ratio of uploads to downloads. Going public or private remains a deeply political issue with arguments supporting either side. Public trackers seek to legitimize and to popularize sharing, where private sites seek to foster a community with standards of participation (see Aitken, 2011).

Over the years since the introduction of BitTorrent torrent search engines have appeared and disappeared – often succumbing to legal pressure or general obscurity[13]. Cooperative local police forces aided in closing sites facilitating piracy. SuprNova, one of the first torrent search engines on the Internet, shut down without going to court in its native Slovenia. Instead, its administrator decided to close the site after having his server confiscated by the police and he felt closing the site was in his best interest. Finnish torrent site, Finreactor, did go to trial, but the courts rejected the defence's claim that the site was not responsible for the copyright infringement because they knew pirated goods were being shared and they did nothing to prevent piracy (Aughton, 2006). Beyond any argument or technical trick, the group benefitted from the loose Swedish laws, at the time, around peer-to-peer and file sharing that allowed them to run a BitTorrent tracker and search engine without breaking the law. Given the upsets in the world of search engines, the longevity of Pirate Bay appears to have contributed to the growth and popularity of BitTorrent.

The Pirate Bay proved to be one of the most popular BitTorrent sites on the Internet since its launch in 2003. It has endured longer than any other unfiltered BitTorrent tracker and search engine. As of July 2012, The Pirate Bay reports it has 5,827,346 registered users sharing 4,373,866 torrents. The site has seen tremendous growth as seen in Figure 14. The figure aggregates the number of users, peers and torrents listed on The Pirate Bay since 2000. The

[13] Wikipedia keeps an excellent list of BitTorrent sites that have shuttered over the years. The list is found here: http://en.wikipedia.org/wiki/Legal_issues_with_BitTorrent.

data comes from the records of Archive.org. The site administrators estimated that half of Sweden's Internet traffic flows through their trackers. To keep up with the demand at its height, the site ran over thirty servers, five dedicated to running the website and sixteen servers facilitating peer-to-peer sharing. Their servers all ran free software using Linux as an operating system, OpenTacker to track torrents and Lighttpd as a web server. Each server responds to 10,000 to 20,000 connections per second. The administrators modified much of the software's code to keep up with this demand; something that would not be possible without open source software (Sunde, n.d.).

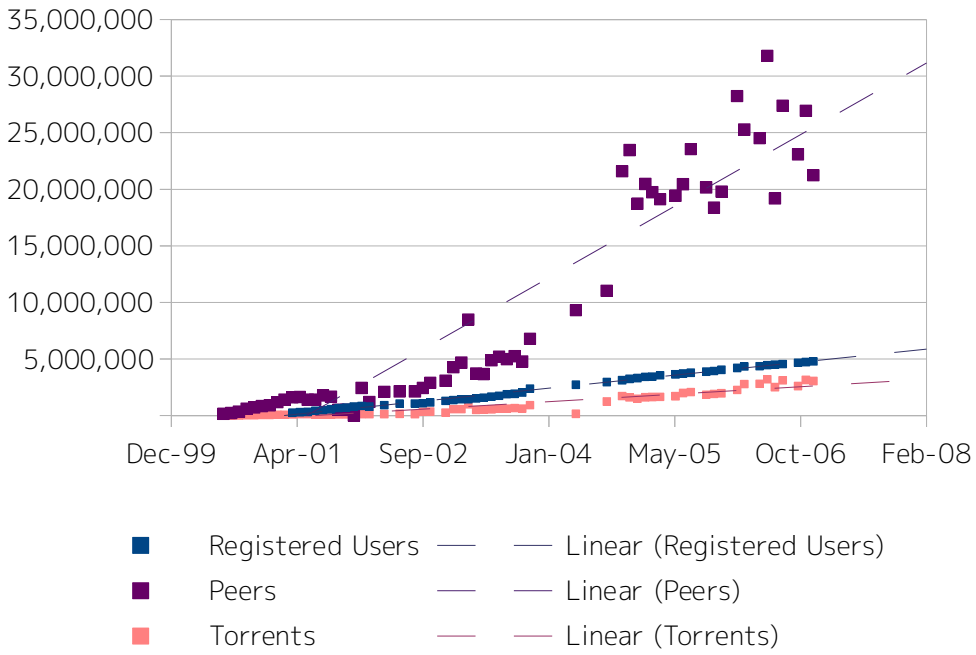


Figure 14: Growth of The Pirate Bay

The traffic also gave The Pirate Bay greater political influence that they leveraged to become a critic of copyright and a proponent of free copying. Andersson describes their politics as "a publicly visible stance, supportive of unrestricted file-sharing" (2009, p. 66). The administrators kept the site as open as possible. TPB did not censor any of the torrents on

their server. Peter says, "we have created an empty site where the only condition was that you cannot upload something where content doesn't match the description or if it blatantly is criminal in Sweden" (B. Jones, 2007, np.). Elsewhere he says, "we have a strong policy at TPB that we do not censor anything" (Sunde, n.d., np.).

The Pirate Bay had a global impact. Neij described a 2006 business trip to San Francisco, when, "there was a school class lined up outside a museum, a big group of eight- or nine-year-old American kids. And a bunch of them started pointing at me: 'Hey! Pirate Bay! Cool'" (Daly, 2007, np.). After they noticed Neij wearing a Pirate Bay t-shirt. They promote a philosophy of *kopimi* or copy me. Kopimism argued file-sharing is copying, not theft, since digital circulation allows for mass duplication. In their manifesto entitled POwer, NET SECRET, Broccoli and KOPIMI, The Pirate Bay offers its readers 109 slogans. Though the absurd, controversial and political tone of the manifesto resists any *one* reading, it clearly embraces kopimism. It encourages its readers to "/join #kopimi", to "upload", to "invent or misuse Kopimi" and to "share files with anyone who wants" (The Pirate Bay, 2011). Kopimism became an official religion in Sweden in 2012 after the Church of Kopimism successfully lobbied the Swedish government to be recognized as an official church (Fiveash, 2012). The spread of kopimism is just one example of the rule of The Pirate Bay in the global Piracy movement.

Proponents of kopimism suggest P2P networks are a grey commons, something different from the legal commons as promoted in the Creative Commons movement (Fleischer & Palle, 2007; Fleisher, 2008). The grey adjective stresses the ambiguity of content on the site. Legality it rests "between the penguin white of a creative commons license and the pitch black of a zero day blockbuster release" (Fleischer, 2006, np.). Greyness hints at the fugitive networks of P2P that seek to avoid a central control that might dictate licit and illicit on the network; rather, it seeks the expansion and growth of the network without concern of its con-

tent. The grey commons is a place where "a space of production, of inspiration, obtaining, downloading – remixing and reinserting distribution and up-down-loading of data"(Fleischer & Palle, 2007, np.). TPB fostered the grey commons by avoiding and central policing of content.

Not only did they avoid censoring or limiting the growth of the grey commons, they actively worked to expand and sustain it. In 22 August 2007, TPB administrators re-launched the once-popular SuprNova.org. The takedown of Suprnova was a major blow to online piracy and one of the first takedowns of a torrent site. After its closure, the administrator gave the domain name to TPB who re-launched the site on their own servers. When the site went back online, its front-page proclaimed:

> Finally, some words for non-internet loving companies: This is how it works. Whatever you sink, we build back up. Whomever you sue, ten new pirates are recruited. Wherever you go, we are already ahead of you. You are the past and the forgotten, we are the internet and the future.

All these tactics seek to advance a kind of accelerationism without any set boundaries or direction using BitTorrent. This strategy of unfettered growth eventually came to an end as the law finally apprehended The Pirate Bay.

The bulk of TPB legal problems began in May 2006 when police forces raided TPB and confiscated its fifteen servers[14] and arresting three people. Soon after the takedown, the Motion Pictures Association of America (MPAA) released a statement celebrating the takedown of the site. Reports later indicated that the takedown occurred after international groups, specifically the MPAA, pressured the Swedish government and police into action

[14] One of these servers now resides in the Swedish National Museum of Science and Technology. See: http://www.tekniskamuseet.se/1/259.en.html.

(Daly, 2007; Moya, 2008). TPB was back online three days later once the police released the administrators after questioning. The raid catalyzed the Swedish community around the group and fostered the nascent Pirate movement. Swedish youth who grew up with computers and digital networks began to politically engage in response to the raid. While the Pirate Party started on 13 February 2006 after the Swedish authorities approved the 1,500 handwritten signatures necessary to add its name to the ballot, the police raid shored up part members as youth expressed their outrage and pushed the party into the public spotlight (Burkart, 2012; Miegel & Olsson, 2008). The police proceeded with their case and filed charged on 31 January 2008, two years after the raid. The trial began a year later on 16 February 2009 and ended in November after the group lost their final appeals. The Swedish court found them guilty. The three administrators have been sentenced to roughly a year of jail time and fines totally $6.5 million dollars (Ernesto, 2010b; Kiss, 2009). Losing the court cases did not shut down the website as the Swedish Pirate Party began to host the site (Lindgren & Linde, 2012, pp. 148–149) and continue to carry traffic to the site although it seems The Pirate Bay continues to manage its own servers (Ernesto, 2011b). Even though the site continues to exist, it has become threatened by the traffic management software discussed in the last chapter.

Mid-way through the case, however, advances in transmissive control became the next major threat to P2P. Indeed, as The Pirate Bay stood in Swedish courts, Internet Service Providers in Canada stood before the CRTC to explain their traffic management of P2P traffic (Canadian Radio-television and Telecommunications Commission, 2009b). Rogers later disclosed they used Deep Packet Inspection software at the time to limit all P2P file sharing uploading to a maximum of 80 kbps (Rogers Communications, 2012) and Bell Internet clearly stated they throttled BitTorrent, Gnutella, Limewire, Kazaa, eDonkey, eMule and WinMX traffic on residential networks. Throttling limits download speed to 512 kbps download speed

from 4:30pm to 6:00pm daily and down further to 256 kbps after 6:00pm. The caps later rise at 1:00am back to 512 kbps before being turned off after 2:00 am (Bell Canada, 2009b). Their usage of transmissive control indicates that struggles against piracy have moved away from the court room into the network. Now ISPs install plug-and-play appliances that append the Internet's running code, so that the software routing packets on the network also hunts for patterns of piracy. As a result, the hunt becomes all the more inescapable for piracy as the line of acceleration has been captured by new forms of transmissive control. The following section describes this change to understand the need to change tactics away from accelerationism.

The Packeteer 8500 and Escalationism

Fashioned at last into an arrowy shape and welded by Perth to the shank, the steel soon pointed the end of the iron; and as the blacksmith was about giving the barbs their final heat, prior to tempering them, he cried to Ahab to place the water-cask near.

"No, no - no water for that; I want it of the true death-temper. Ahoy, there! Tashtego, Queequeg, Daggoo! What say ye, pagans! Will ye give me as much blood as will cover this barb?" holding it high up. A cluster of dark nods replied, Yes. Three punctures were made in the heathen flesh and the White Whale's barbs were then tempered."

Ego non baptizo te in nomine patris, sed in nomine diaboli!" deliriously howled Ahab, as the malignant iron scorchingly devoured the baptismal blood.

Long into the search for the While Whale and in the waters around the equator, Ahab commands the smith to forge a new harpoon. He brings with him razors that become barbs to decorate the iron, so it will catch in the body of the Whale. His deepening madness – usually hidden behind the door to his cabin – taunts the smith and commands the ship's harpooners to drench the newly-forged arrow in their own blood. A baptism, as Melville describes it, "in nomine diaboli" or in the name of the devil. To pirates, traffic management software represent a similar menacing weapon designed to recognize and control patterns of P2P networking. Many different firms offered these types of weapons. This chapter was able to get access to

one such device, a Packeteer 8500 seen in Figure 15. The following section offers a thick description of its interface and its techniques to control traffic[15].

Figure 15: The Packeteer 8500 studied in this chapter.

The Packeteer was first released 2002 and it is exemplary of the kinds the new weapons hunting piracy and The Pirate Bay. Packeteer led the field in advanced traffic management software since its founding in 1996 until its acquisition by BlueCoat[16] in 2008 (Lawson, 2008). The PacketShaper 8500 was the most robust appliance in their product line because it could handle 200 megabits per second to delineate a maximum of 500,000 IP flows into over 5,000 classes, partitions or policies. A pamphlet for the product suggests "It's the answer to service

[15] The study wishes to acknowledge the generous support of Ryerson Computing and Communication Services. In particular, this research would not be possible without the assistance of Ken Woo and Ken Connell who helped set-up the testing lab, access to the Packeteer PacketShaper 8500 and answered countless questions about its operation.

[16] When Hacktivists Telecomix leaked censorship logs from Syria, some of the logs came from BlueCoat SG-9000 HTTP proxies filtering the web for the government. See: http://yro.slashdot.org/story/11/10/05/1249209/telecomix-releases-54gb-of-syrian-censorship-logs.

providers' demands for a high-capacity solution that delivers differentiated services, ensures fair and equal access, enforces user policies and improves profit margins through various co-location services" (Packeteer, Inc., 2001, p. 1). A review of the newly launched project states that "the largest demographic for peer-to-per file sharing in college students" and that the PacketShaper is a serious asset "in a university environment, where protocols such as those associated with Kazaa and Gnutella are clogging up the pipes;" however, peer-to-peer protocols "disguise themselves via HTTP tunnelling or using multiple ports" – a phenomenon explained in Chapter Three as port spoofing. To compensate, the review continues, the PacketShaper "looks at more than just port number. Instead, it examines application signatures" (DeMaria, 2002, p. 22). Appliances, like PacketShaper, arrived as weapons to hunt P2P networks – weapons that would be intelligent enough to adapt and respond to the accelerationism.

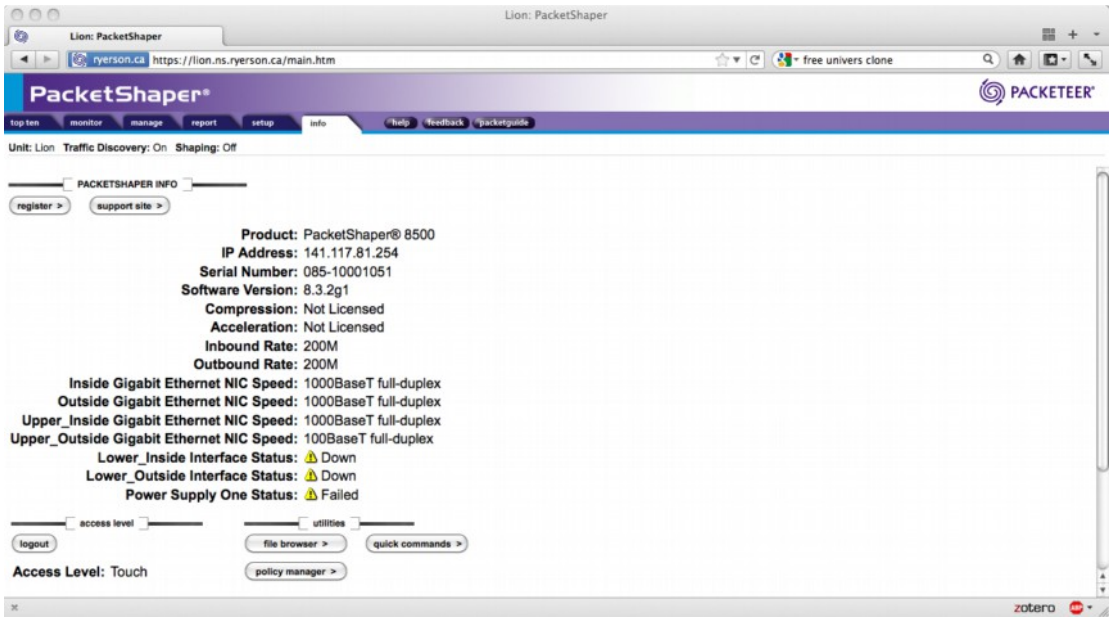


Figure 16: The PacketShaper 8500 interface

The Packeteer 8500 installs directly into a standard network rack, where an administrator could insert the software as another hop in flow of packets. Once installed, the box could be administered by a web interface as depicted in Figure 16. It includes ways to classify and manage IP patterns, indications of the perspective and logics of its algorithms. It classifies traffic into classes that correspond with Internet applications Skype or HTTP both have their own traffic class. The class-based perspective of the PacketShaper, seen in Figure 17, consists of a tree of traffic classes grouped into Inbound and Outbound. It, as the manual states, "displays applications in a hierarchical tree representing application traffic traveling inbound and outbound" (Packeteer, Inc., 2002, pp. 6–2). Where a class resides in the Tree corresponds to when the PacketShaper will process its rules. Like a hand moving down a list, the PacketShaper runs through the tree from top to bottom, matching information in a packet to patterns in classes. The Tree changes as administrators add classes or when PacketLogic updates its software. Most vendors release updates that add new classes based on their own monitoring of traffic pattern trends. The Application Tree also automatically adds classes when set to Traffic Discovery mode. The automated mode searches for repeating traffic patterns and creates new classes after its recognizes the same pattern three times. A network administrator might leave the appliance in Discovery mode for a week or so to generate a list of popular applications before turning it off and letting it run.

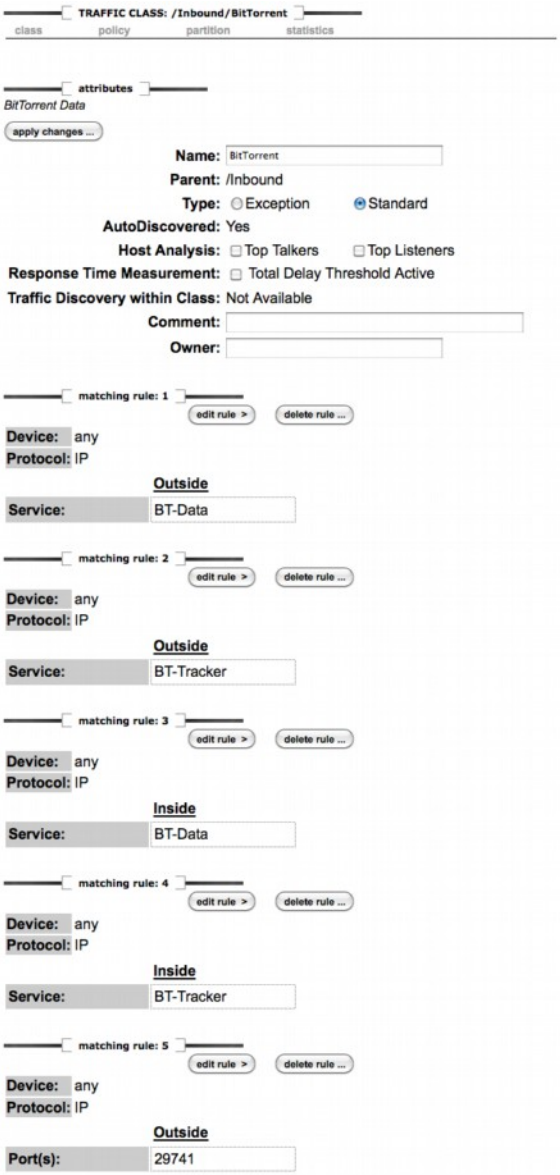


Figure 17: A BitTorrent Traffic Class in the PacketShaper 8500

Each traffic class includes a list of rules for the PacketShaper to follow to identify a packet. The BitTorrent class, for example, lists 5 rules, seen in Figure 17. Rules, in this case, question whether a packet contains BitTorrent Data or data to a BitTorrent tracker.

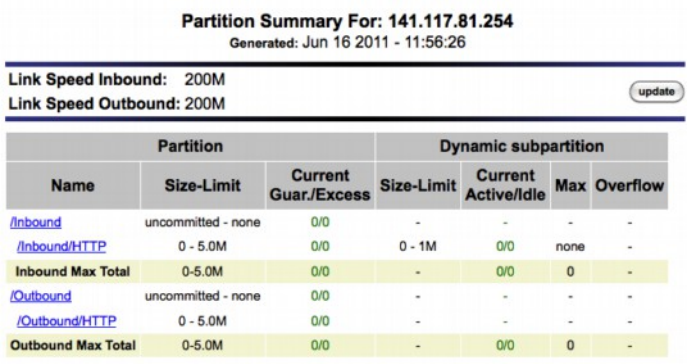
Unfortunately, a closer inspection of any rule offers little guidance to its actual operation. The rule selects one of a few options from a drop down menu, such as BT-Tracker. An admin-

istrator can add rules to a box based on port numbers or IP address. Buried at the bottom of the rule page, the help text admits that the PacketShaper allow for a few application-specific matching rules attachable to classes. While some of its features refer to fairly specific classes such as databases (PostgreSQL or Oracle), it also contains application-specific rules for HTTP, FTP and NNTP. HTTP criteria can filter according to URL, content type or browser. Hypothetically, it could block traffic from users of Firefox browsing The Pirate Bay and downloading torrent files, while allowing all other HTTP traffic to flow normally. FTP criteria includes file names or extensions. The interface help manual suggests, "for example, to classify FTP downloads of MP3 files, you can specify *.mp3 as the File Name criterion". Finally, NNTP, the Network News Transfer Protocol popular for UseNet allows for the classification of group name, a feature capable of blocking the binary groups that are havens for pirated content.

Since the PacketLogic software is closed source software, a deeper reading of its code is not possible; however, iPoque, another vender of traffic management appliances, has opened a portion of their code as the OpenDPI project and a reading of this code expands the operation of advanced traffic management detection. The source code, listed in Appendix 4.2, consists of code for a program to detect BitTorrent traffic. Its one of many files in the source code to recognize certain patterns for different applications such as *World of Warcraft*, Kazaa and BitTorrent. This pattern-recognition code appears to correspond with the classes built into the PacketShaper. The code of the BitTorrent.c file, for example, lists a set of rules to detect a BitTorrent packet. It contains a series of functions that use the packet as an input. The program runs down the list of functions before classifying traffic as BitTorrent. It checks, for example, for a "plain webseed BitTorrent protocol" by looking at the packet length and the payload to see if it contains "GET /webseed?info_hash=". The code is, in short, a series of patterns associated with BitTorrent that OpenDPI looks for in the packet. No doubt, the Packet-

Shaper would employ a similar technique as hinted at by the different ways it classifies BitTorrent traffic.

Once identified, the PacketShaper has two general logics to manage networking: policies and partitions. Both refer to certain logics for the software to follow when encountering packets of a certain class. Policies, according to the manual, manages individual flows, where a partition manages aggregated flows. A difference, in other words, concerning the granularity where a policy allows a network to "to manage bandwidth on a flow-by-flow basis" and a partition groups flows "so that all of the flows for the class are controlled together as one" (Packeteer, Inc., 2002, pp. 6–6). A policy could apply to HTTP, where HTTP could also be part of a partition that also include FTP and Email. The manual suggests creating rules protecting "mission-critical" traffic, while shaping "aggressive traffic" While the perspective of these two logics may differ, they both have the same resources in managing traffic. Their capacities roughly correspond with the types of application requirements outline by Tanenbaum (2002) in the last chapter. Policies and partitions can guarantee a bit rate, set the priority in the queue, pass the traffic through the network, impose DiffServ or MPLS or block traffic altogether. The policies could simultaneously block malicious content, ignore normal activities so it travels according to best efforts and guarantee bitrates for value-added traffic. The most common function would be to guarantee a minimum and maximum bitrate to ensure proper application functionality. Along with guarantees, a policy might also allow a flow to burst – that is to temporarily send more bit than it rates – according to a priority and a limit. Priority, as discussed in Chapter Three, refers to the queue of the PacketShaper. While the policy offers a number of options, partitions offer a more common solution.



Partition Summary For: 141.117.81.254
Generated: Jun 16 2011 - 11:56:26

Link Speed Inbound: 200M
Link Speed Outbound: 200M

update

Partition			Dynamic subpartition			
Name	Size-Limit	Current Guar./Excess	Size-Limit	Current Active/Idle	Max	Overflow
/Inbound	uncommitted - none	0/0	-	-	-	-
/Inbound/HTTP	0 - 5.0M	0/0	0 - 1M	0/0	none	-
Inbound Max Total	0-5.0M	0/0	-	0/0	0	-
/Outbound	uncommitted - none	0/0	-	-	-	-
/Outbound/HTTP	0 - 5.0M	0/0	-	-	-	-
Outbound Max Total	0-5.0M	0/0	-	0/0	0	-

Figure 18: A partition summary

A partition, like a slice of pie, divides the available bandwidth into sections that have a fixed capacity. The partition summary, seen in Figure 18, list the various active partitions. As seen, Inbound/HTTP has been limited to 5.0Mbps. With the partition menu, an application might be able to be burstable up to a certain bitrate. Beyond bitrates, a partition also can dynamically create smaller partitions when nodes on the network begin using an application. Nodes refer to either a single IP addresses or groups of IP addresses known as a subnet. A sub-partition manages how nodes shares a fixed amount of bandwidth either through simple division or through set amounts. A user might be able to receive 30kbps in a sub-partition of 1.5 Mbps until there is not enough bandwidth for all to receive that rate and the partition begins offering less bandwidth. Components, classes, policies and partitions form the building blocks of a temporal economy using a PacketShaper. What makes the PacketShaper a significant technology is the capacity of creating a complex system of policies and traffic management, not necessarily the ability of creating any one rule. Constructing tiers for traffic cluster applications and bitrates together. The PacketShaper represents a machine of transmissive control capable of a modulating influence that supports the production of temporal economies of Internet traffic.

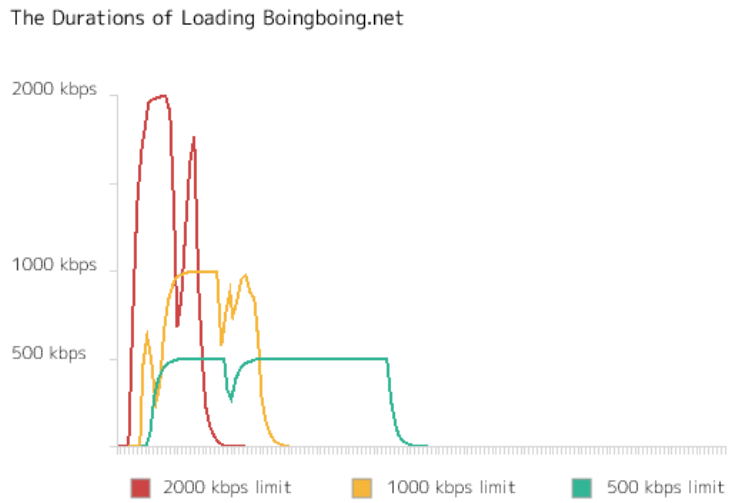


Figure 19: Multiple Load Times

Figure 19 depicts the change in the load time of the popular blog BoingBoing.net. Lowering the partition cap in the PacketShaper raises the load time of the website. A cap of 2,000 kpbs loads the site in seconds, where a cap of 500 kpbs stretches the load time to almost a minute. The simple test demonstrates how transmissive control alters the durations of a loading the same website.

With a PacketShaper, an ISP creates tiers of subscribers who play for access to these constructed zones of communicability. Figure 20 illustrates the production of a simple tiering of traffic. Three partitions were created – one for YouTube (green), HTTP (blue) and BitTorrent (red) with maximum bitrates respectively set at 100 kbps, 75 kbps and 50 kbps. The chart on the left depicts a computer simultaneously downloading Ubuntu through the web, through BitTorrent and watching a movie on YouTube. HTTP peaks at over 60M per second without shaping, but, on the right, its lines cap at its partition limit. As a result the file will take longer, but will be comparatively faster than BitTorrent or YouTube.

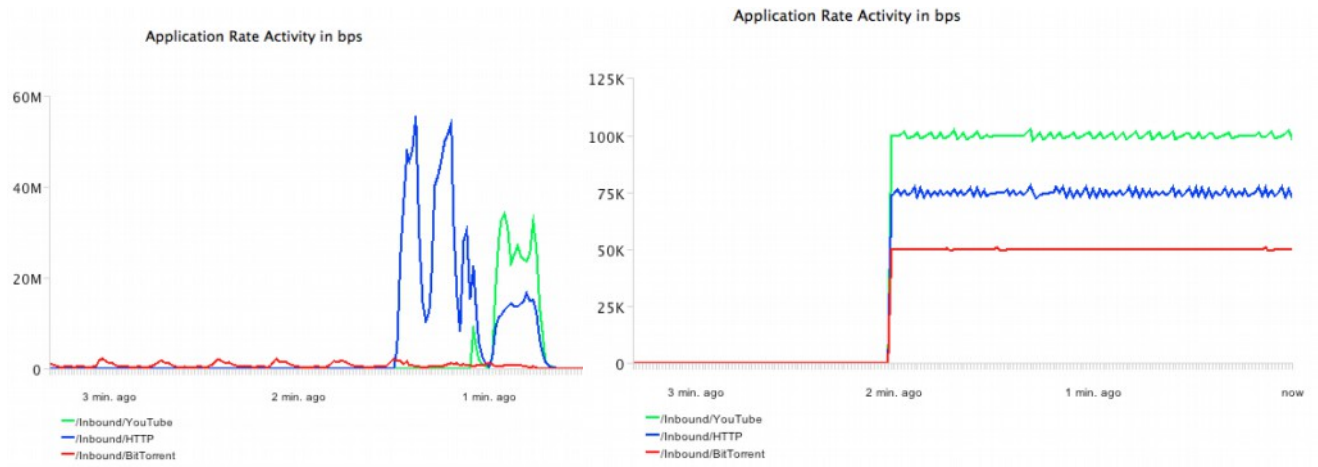


Figure 20: Creating tiers using the PacketShaper

This capacity, however, has its limits as the PacketShaper cannot handle traffic greater than 200 mbps, 500,000 flows or 5,000 policies and partitions. Since many networks routinely use more than 200 Mbps, the software clearly has its limits. These limits concern the modulations of a PacketShaper, how flexibility and adaptability of its software to new and numerous traffic flows. Hypothetically, the PacketShaper 8500 would not be able to create a temporal economy with more than 5,000 rules that would configure the relations between traffic flows. This remains a hypothetical limit, firstly, because most ISPs use simpler regimes of passage and, second, newer PacketShapers, such as the Procera PL10000, can shape up to more than a 120 Gigabytes of traffic per second (Procera Networks, n.d.). These challenges, as will be discussed in the following sections, have more to do with the limitations of the PacketShaper 8500 than with the rapidly advancing DPI market (Sherrington, 2011).

With the rise of the advanced traffic management came a need to re-think the tactics of accelerationism. Is going faster no longer answer? As early as 2006, one of its members Neij admitted, "The Pirate Bay will outlive its usefulness" (Norton, 2006, np.) Traffic management algorithms put an end to a strategy of accelerationsm as there is nowhere to run. The network

itself can continually adapt to new networks. Every node, every path is subject to the same transmissive control. The ubiquity of control requires a new strategy. Deleuze suggests the following way out,

> Maybe speech and communication have been corrupted. They're thoroughly permeated by money – and not by accident but by their very nature. We've got to hijack speech. Creating has always been something different from communicating. The key thing may be to create vacuoles of noncommunication, circuit breakers, so we can elude control. (1995a, p. 175)

The idea of non-communication might not mean simply to stop, but, rather to question the very expression of communication. Deleuze (1998a) defines communication as the transmission of information or order-words. To stop communicating would not be to stop talking, but to stop the widespread distribution of an information system or, to Deleuze, a system of control. Given the ubiquity of transmissive control, fleeing toward an outside no longer seems viable. Accelerating assumes a free horizon, whereas, Deleuze suggests the creation of a vacuole – a term from the Latin vacu-us meaning an empty or open space. The production of these space, he suggests, would elude control – a translation French verb *échapper* that could also be translated as to escape, to dodge or to run away[17]. How might one create vacuoles of noncommunication to elude control?

Escalationism, as Fleischer (2010) suggests, might be the kind of move Deleuze imagines to replace accelerationism by creating vacuoles of non-communication. Fleischer, reflecting on the end of a politics of acceleration writes, "in 2010, we are tunnelling communications"(2010, np.). By tunnelling communication, he means both an analogy of tunnelling underground to avoid detection and a technical term to refer to routing communications through encrypted

[17] For the original French interview, see http://multitudes.samizdat.net/Le-devenir-revolutionnaire-et-les.

or obscure channels. His phrase then refers to a growing awareness of escalation of networking and avoiding disastrous escalations. Constructing darknets – private obscure networks on the Internet – exemplifies the escalationism strategy. He compares dark nets to the strategies of an open P2P search engine,

> we have been talking about darknets at least since 2005. But for long, we tended to present darknets only as the less preferable alternative to open P2P-networks. If openness was associated with the famous "long tail", we speculated that attacks on open sharing would not stop sharing but force it into smaller and darker networks of trust, which could limit access to the very mainstream of music and movie files. This theory probably still bears some truth, but seems to be just one tiny part of a larger complex. In the end, many of us use virtual private networks and access our IRC communities via SSH on a daily basis. Darknets for data do not need to use the internet infrastructure, but when they do, they have the character of an internet-in-the-internet. The most radically anonymous darknet experiments, like I2P, does not even have any gateways to the "ordinary" internet, but operates in tunnels underneath – slooowly. (Fleischer, 2010, np.)

Tunnelled communications do not participate in the same communications systems deploying tiered transmissive economies. If one strategy of the whale is to swim away, another might be to dive, deep and away from the eyes of its hunters. The Pirate Bay, as well, recognized the need to change course and their efforts mark the final body in this chapter.

Escalationism and iPredator

And thus, through the serene tranquillities of the tropical sea, among waves whose hand-clappings were suspended by exceeding rapture, Moby-Dick moved on, still withholding from sight the full terrors of his submerged trunk, entirely hiding the wrenched hideousness of his jaw. But soon the fore part of him

slowly rose from the water; for an instant his whole marbleized body formed a high arch, like Virginia's Natural Bridge and warningly waving his bannered flukes in the air, the grand god revealed himself, sounded and went out of sight. Hoveringly halting and dipping on the wing, the white sea-fowls longingly lingered over the agitated pool that he left.

When the crew of the *Pequod* finally encounters Moby-Dick, the whale is more menacing and unpredictable than even the depths of Ahab's mind. It does not flee, but rather it dives. Deep into the black abyss of the sea where it lingers outside the sight (but always in the minds) of the whalers, until it rises to smash through boats and upset the seas around them. From the depths, the whale smashes against the sides of the *Peqoud* and dodges the harpoons of Ahab. Depth through the dive echoes the second escalationist line of flight. Networks, armed with PacketShapers and other machines of transmissive control, have a terrible arsenal to stop piracy and P2P. Faced with new harpoons of traffic management, The Pirate Bay also changes tactics from outrunning to bunkering down. A new form of transmissive control offers the group a means to dive away from their hunters – a Virtual Private Networking (VPN) service known as iPredator. The following section thus offers an account of the operation of iPredator and how it embodies a pattern of escalationism on the Internet.

The Pirate Bay launched their iPredator service in response to changes in Swedish law in 2009. On 1 April 2009, the Swedish government ratified Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, (also known as "Intellectual Property Rights Enforcement Directive" or "IPRED") in 2009 (Cheng, 2009). The introduction of IPRED closed the loop holes that allowed The Pirate Bay to operate legally in Sweden. It further allowed for greater police monitoring of the Internet. Its introduction marks a change in the tactics of The Pirate Bay. TPB's iPredator, a name mocking the IPRED directive, is a VPN service that aimed to shelter its clients' Internet traffic from surveillance and throttling by traffic shapers. They announced the

service on the homepage of The Pirate Bay by changing their logo to Figure 21. It is a screen-shot from Nintendo's Punch-Out where its protagonist Little Mac fights Glass Joe, an earlier opponent easily defeated due to his characteristic glass jaw. Peter Sunde says iPredator sought "to hide from what the government does in the form of giving companies police powers" (Tay, 2009, np.). Even though the administrators were still fighting their legal trial, they expanded the fight to protect an open Internet.

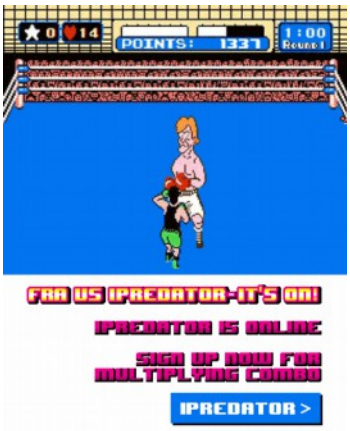


Figure 21: Pirate Bay doodle announcing iPredator

The service is a virtual private network (VPN) that creates a secure and private connection between a home user and the iPredator's servers. In effect, iPredator allows its users to tunnel their communications to cloak it from the perspective of PacketShapers. The service costs 5 euros a month. Virtual private network technology establishes a private network on the common lines of the Internet. Researchers at AT&T in the USA and the UK proposed VPNs in 1988 as a way for to provide "business with the features and flexibility of the private network, while leaving the maintenance and operational aspects to the [public switched telephone network] operator" (Wood, Stoss, Chan-Lizardo, Papacostas, & Stinson, 1988, p. 1). While they proposed the VPN over telephone networks, the Internet soon eclipsed private networks, firms gradually moved away from leasing physical private lines to virtually creating private

lines through VPNs. A number of VPN protocols developed over time including PPTP, IPSEC, PPPoE, OpenVPN and L2TP (Snader, 2005).

While it claims to be making the switch to the GPL-licensed OpenVPN, iPredator continues to use the Point-to-Point Tunnelling Protocol (PPTP). PPTP basically establishes a direct link between a client server and a VPN server. All traffic from the client – a request to website for example – flows from the client to the VPN servers, out to the Internet and back to the VPN server where it returns the information to the client. The protocol emerged out of research by a consortium of companies, including Microsoft and 3Com, that cumulated in RFC 2637 posted in July 1999 (Hamzeh et al., 1999). The protocol encapsulates traffic originating from a client. Encapsulation is a term designating when a protocol higher up the IP stack encodes the data of another protocol; it is a ubiquitous term in IP as the Link Layer Protocols always encapsulates Application Later protocols. In the case of PPTP, the VPN uses the PPTP and GRE protocols to enclose around the message to protect the message from inspection by networks ferrying packets between the client and the VPN server (Snader, 2005, pp. 85–93). According to Snader, PPTP is more accurately seen as a way to tunnel information to avoid inspection than to establish a complex network (2005, p. 131). While the protocol does not outline any encryption for its tunnelling, iPredator uses 128-bit encryption using Microsoft Point-to-Point Encryption for traffic and Microsoft Challenge Handshake Authentication Protocol for to log into the VPN (Patowary, 2010).

While iPredator technology might be fairly conventional, it has a decidedly political implementation. The company incorporated in Sweden. The firm Trygghetsbolaget i Lund AB, a firm who has worked with the Pirate Party in the past to create political VPNs, handles their VPN services. It operates as a "pre-paid flat-rate service" because this business model, they claim, has the lowest reporting requirements since they do not have to log and charge for

usage. iPredator does not keep logs of user since IPRED does not mandate data retention (Tay, 2009). Their security page claims that they will cooperate with Swedish authorities only if a user may be facing jail time. Their website claims that for "inquires from other parties than Swedish authorities iPredator will never hand over any kind of information"[18]. Given that their service attracts international customers, they again appear to be playing international laws to their advantage, forcing international legal co-operation before releasing any data to the local authorities of an international user.

A VPN service, much like a P2P network, is a form of E2E transmissive control countering the QoS algorithms employed by the ISPs. iPredator acts as the intermediary transmitter between its clients and the Internet and, in doing so, re-routes the connection to networks managed by The Pirate Bay. As these iPredator home page once stated, "the network is under our control. not theirs". Re-routing packets through Sweden disrupts the geo-targeting used by advertisers for example. Since content providers never know the actual IP address of their targets, advertisements and other customization target for the wrong local. Targeted advertisements on Facebook read in Swedish. Only iPredator knows the connection between its clients and their destinations. Their servers do not log the relation longer than necessary for their programs to complete the routing. In short, changing the flow of the packets disrupts the operation of network algorithms that rely on knowing both the source and destination.

Experiments in the test lab help explore how iPredator eludes the Packeteer. Its interface offers a window into this quest through its real-time charting of packet flows. It easily detects BitTorrent traffic. A first test used version 5.2.2 of the BitTorrent client from roughly 2009. The version corresponds to the type of BitTorrent traffic that Packeteer had built into its pro-

[18] The website does not provide an author or date, but more information about iPredator can be found at: https://ipredator.se/page/about and https://ipredator.se/page/security.

files. The test downloaded a Torrent of the Ubuntu Linux distribution and monitored InBound/BitTorrent and OutBound/BitTorrent traffic through the Packeteer. Downloading Ubuntu hauls the traffic line of the chart from the depths of zero traffic to the heights of megabytes per second. A connection with the more recent uTorrent application (release 2.2.1) gives a similar result. In the span of a simple 3 minute test, uTorrent had downloaded a complete distribution of Ubuntu, 685 megabytes. In this time, the client reported a download speed of 3 megabytes per second and an upload rate of 6 kilobytes per second. The PacketShaper, though not completely accurately, followed the rise of the BitTorrent Inbound traffic (inbound as to the pieces of a file arrive inwards)[19].

Since the PacketShaper easily recognizes BitTorrent traffic, it can just as easily throttle BitTorrent traffic. In the Manage tab, policies or partitions can limit the flow of BitTorrent traffic. For the sake of representation, the test set a partition of 50 kilobytes per second. Waiting until the BitTorrent reaches a rate of 150 kilobytes per second and then engaging shaping pushing the line down until it hits a steady rate of 50 kilobytes per second. The same technique occurs on most commercial networks in Canada that limit the rate of BitTorrent traffic during peak times to ensure it does not congest their networks.

If the application of the PacketShaper to the BitTorrent traffic exemplifies the reach, then iPredator attempts to loosen the PacketShaper's grip on the line. Logging on to iPredator completely alters the flow of packets. Continuing the test from above, when a shaped BitTorrent exchange logs into iPredator, its traffic drops as it changes addresses on the Internet; however, as its location stabilizes and the client re-establishes contacts, the traffic stabilizes

[19] Interestingly, a gap exists between the download rate reported by the PacketShaper and the BitTorrent. After a minute, BitTorrent reports it has established 75 connections with a 104 kilobytes per second download speed and a 3 kilobytes per second upload speed. The PacketShaper, on the other hand, reports a download rate or InBound rate of about 1.5 megabytes per second, while approximately uploading 250 kilobytes per second. Likely this is due to a bug in the version of BitTorrent.

and continues to climb past the set limit of 50 kilobytes per second to well past 400 kilobytes per second. The test duplicates the experience of an iPredator user who seeks to avoid the traffic shaping of its ISP who logs in to iPredator. Importantly though, the speed of iPredator might actually be slower than throttled traffic since traffic has to route through Sweden. The technique would be a mistake in a logic of accelerationism, but its deployment demonstrates the switch toward a strategy of escalationism as it eludes control.

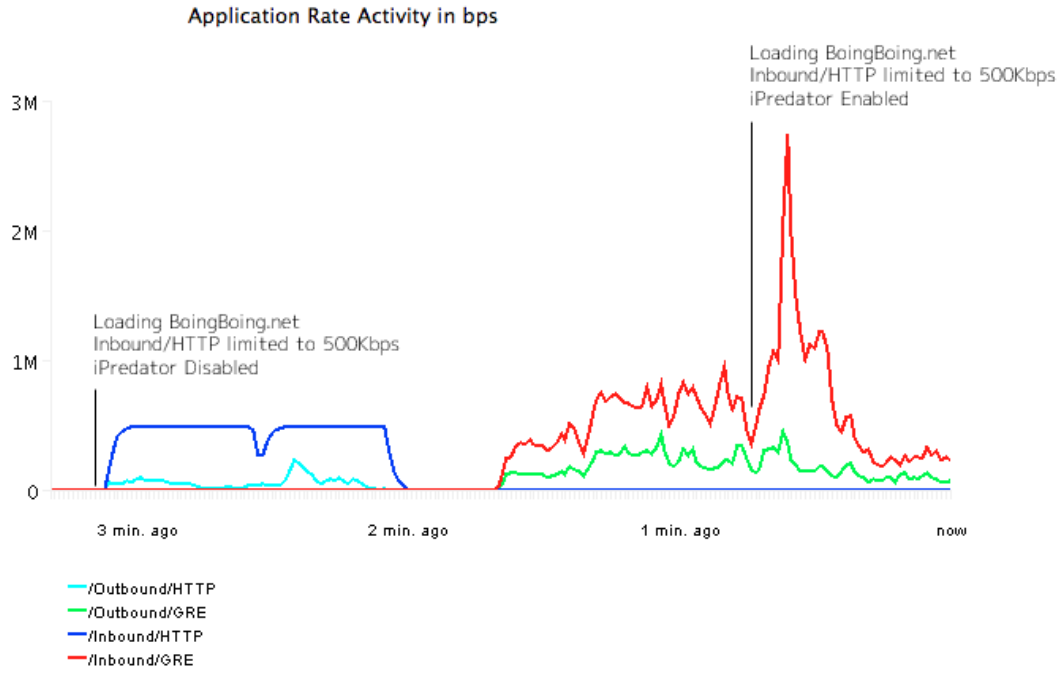


Figure 22: Loading BoingBoing.net with and without iPredator

An example helps explain the activity of the PacketShaper. Figure 22 again depicts the load times of BoingBoing.net. The various lines on the chart depict the types of traffic identified by the PacketShaper. The blue and turquoise lines respectively graph Inbound and Outbound traffic. With a cap of 500kbps, a browsers must wait approximately a minute for the Inbound HTTP traffic to complete loading the website. The browser, incidentally, also com-

municates with the website as well, no doubt to exchange cookies and other commands. Once complete, the test logged into the iPredator VPN. The PacketShaper classified iPredator traffic as Generic Routing Encapsulation (GRE) packets, so the red and green lines respectively depict Inbound and Outbound GRE traffic. After logging in to the VPN, the test reloaded the BoingBoing website. It loaded quicker; more importantly, the PacketShaper no longer classified the traffic as HTTP even though the packets contained HTTP information. PackerShaper no longer applied the cap and the traffic traveled at a higher bitrate (almost always above 1000 kbps). In this case, the escalationist strategy avoided the limits imposed by the PacketShaper.

Using iPredator and the escalationist does not always concern less time through faster speeds. In fact, using iPredator actually slows transmission. Figure 23 compares the SpeedTest broadband without and with iPredator. On the left, the test with the server reaches nearly 80,000 kbps where enabling iPredator results in lessened bitrates. Importantly, the delay does not result from the Swedish traffic having to connect to the United States – a longer distance to travel. SpeedTest has testing servers located in Sweden, so the iPredator-enabled test connects to a Swedish testing server. The advantage of iPredator is obscurity and autonomy, not acceleration. With iPredator enabled, traffic flows according to the relationship between Pirate Bay and the home computer. Deep beneath the surface of an iPredator packet lies its true contents, unbeknownst to the PacketShaper.

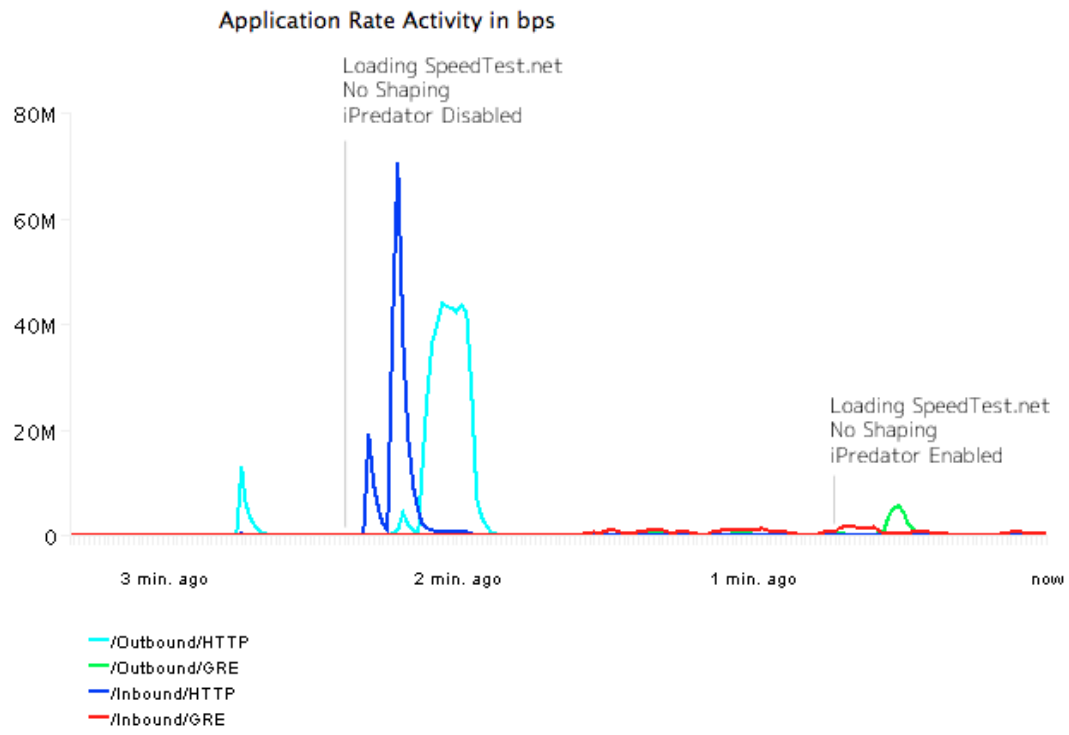


Figure 23: Comparing Speedtest.net

Even though a current policy might not apply to GRE traffic, the PacketShaper still recognizes its tunnelled traffic. The PacketShaper classifies iPredator as InBound/GRE and OutBound/GRE. While the PacketShaper can simply add a new filter to manage GRE traffic, it does so at the risk of also effecting commercial VPN traffic. As introduced prior, iPredator is a form of escalationism, not because it hides the traffic as much as that it hides the traffic among other VPN streams. Most VPN traffic comes from corporations who use it to secure communication between an employee in the field and company servers.

Even though iPredator avoids detection from the Packeteer 8500, new techniques seek to break its encryption or distinguish it from other VPN traffic. The PPTP protocol can be decrypted by eavesdroppers (Tay, 2009). Newer algorithms promise *predictive modelling* that build upon techniques like the PacketShaper and its Traffic Discovery mode to detect encryp-

ted BitTorrent traffic. The Protocol and Application Classification Engine (PACE) by iPoque combines "pattern matching, behavioural, statistical and heuristic analysis" so it is "able to reliably detect proprietary, encrypted and obfuscated protocols with a very low false negative rate and virtually no false positives" (ipoque, 2012, p. 2). PACE is just one example of the new lines of networking applications replacing the PacketShaper that use techniques other than Deep Packet Inspection to classify network traffic. One published algorithm classified encrypted traffic using packer size, arrival time and order to characterize certain applications even though they travelled over secured tunnels such as iPredator. It detected P2P traffic over secure shell (SSH) tunnelling with 88.77% accuracy (Dusi, Crotti, Gringoli, & Salgarelli, 2008). These examples show that escalationism, just like accelerationism, is a temporary solution.

Escalantionism is an emerging pattern among recursive publics, such as pirates, hacktivists and P2P developers, to struggle within, no escape from, a system of control. The Pirate Party of Canada now offers a VPN service to members who donate $10 dollars a month (Ernesto, 2011a). Anonymous and Telecomix, both prominent hacktivist groups, developed secure tunnels and networks connections for dissidents in nation-states with censored regimes, most recently in Egypt and Syria (Greenberg, 2011). Their efforts continue a long history of anti-censorship proxy services. The Citizen Lab created Psiphon[20] to produce secure networks for the Internet without fear of government surveillance. Brunton and Nissenbaum (2011) characterize this trend – what has been called escalationism regarding piracy – as a political tactic of obfuscation, "a counter–logic to data gathering and profile generation" (np.). Obfuscation practices produce "misleading, false or ambiguous data to make data gathering less reliable and therefore less valuable". They categorize various obfuscation practices such as *selective*

[20] For more details about the project see its website: http://psiphon.ca/.

obfuscation that jams data mining by specific sites like Facebook and *ambiguating obfuscation* that "render an individual's data permanently dubious and untrustworthy as a subject of analysis". TPB's iPredator is an example of what they call *cooperative obfuscation* that seeks to collectively obfuscate data collection. The Onion Router, known as TOR, also exemplifies this practice as it creates a distributed network from home nodes who agree to pass information between each other. The relays anonymize and encrypt data, as well, as disrupt the tempo of packet transmission to prevent the kind of flow inspection used to predict the kind of traffic. Another example would be the I2P project that also promises traffic anonymity and security through a similar distributed network. All these projects exemplify that trend of *cooperative obfuscation* identified by Brunton and Nissenbaum. Yet, these strategies not only obfuscate from data collection for surveillance purposes, but indicate an elusion of control mechanisms.

What is at stake is not just personal privacy, but the operation of transmissive that depends on data profiling in its controlled circulation By creating moments or vacuoles without control, escalationist strategies create opportunities for the proliferation and spread of piratical networks and exchanges. The ebb and flow of control and capture illustrate the becoming of the Internet – either as a poly-chronous system of communication with tiers or an unhinged asynchronous medium of all sorts of transmissions with little central control. These struggles form the lines of becoming of the Internet.

The collective becoming of the Internet involves both transmissive control and war machines like The Pirate Bay with its lines of flight. Their political struggle then involves a modulation of control and its elusion. The virtualities of control adapt their modulations in response to the lines of flight. How long do lines of flight disrupt transmission and temporal economies? Lines of flight are only temporary victories as they prompt new modulations of algorithms. Where network routers now easily manage P2P traffic, they still do not possess the

depth to read VPN traffic. For now, The Pirate Bay eludes control through iPredator. While the techniques elude routine control, new Deep Packet Inspection, as previously mentioned, increase the perspective of network control algorithms to compensate for falsifying IP headers. Companies now sell software that can inspect packets even if these packets employ port spoofing or encryption.

Conclusion

Resolute and unmoved, Ahab answers: "Ahab is forever Ahab, man. This whole act's immutably decreed. `Twas rehearsed by thee and me a billion years before this ocean rolled. Fool! I am the Fates' lieutenant; I act under orders. Look thou, underling! that thou obeyest mine." Thus, in delusions of grandeur, the chase continues.

Two days into the hunt and two fleeting encounters with the white whale leave the crew tired and disparate. Starbuck, the First Mate, begs Ahab to relinquish the quest and to give up the hunt for the sake of the crew and the ship. Even though Captain and First Mate have bonded close during the voyage, Ahab remains steadfast in his hunt for the whale. He has come to know his fate, a destiny. As Deleuze and Guattari write, "Captain Ahab says to his first mate: I have no personal history with Moby-Dick, no revenge to take, any more than I have a myth to play out; but I do have a becoming!" (1987, p. 245). Ahab and his hunt for the White Whale captured the becoming of a poly-chronous Internet; yet, the romanticism of the hunt in part drives on the intensification of forms of control. "Ahab is forever Ahab, man". He hunts through the night, with a singular desire. Giving him chase only spurs him on further. The hunt will always continue. It has been played out through countless versions of P2P. Each line of flights ends in its captures, with transmissive control stronger, with a more crystalline vision of the optimal temporal economy of the Internet. The double helix of the Internet's DNA

twists forever onward. Its curves are rich with the perpetual interplay between communication and control.

Lines provide the theoretical concepts to understand the becoming of the Internet through the struggle between piracy and transmissive control. Three lines appear in this chapter. The segmented line of packets provide a smooth space for control. Supple lines align packets with their temporal economies. By manipulating and managing segmented lines, the supple lines express a direction and specific becoming of the networks. It is these lines that express temporal economies. A third line haunts an assemblage: the line of flight. Nomadic war machines, such as The Pirate Bay, produce these lines of flight. Both accelerationism and escalationism are lines of flight in their attempts to elude control and to find new forms of networking. The interplay between these three lines characterize the future of the Internetlike the lines of the *Pequod* and Ahab chart across the globe in his quest for the White Whale. These concepts offer a means to understand piracy in its escape from transmissive control.

Innovations by The Pirate Bay threaten to strengthen and improve transmissive control precisely because they attempt to elude it. Control grows through opposition. Burroughs, whose writings on control inspired Deleuze, recognized that the limits of control are as much a part of the system as control itself. He recognized that "control needs oppositions or acquiescence otherwise it ceases to be control" (2000, p. 339). The lines of The Pirate Bay injects a productivity into the Internet. Just as Ahab's quest for the unknowable white whale drove him to becoming something else, network owners find a productivity in their hunt for piracy. In a way the networks have begun their own quest, beyond the hunt – their goal is a new network beyond The Pirate Bay without the need of their threat, they have found new threats of cyber-terrorism and lawful access. Tools once developed to control piracy, now promise to rewire networks entirely. Transmissive control is now beyond piracy. Their hunt resembles the

hunt of Ahab and his break with the whalers' pact. In the end, the hunt is more about the becoming of Ahab then actually the white whale. Transmissive control has moved past simply hunting for piracy and beyond The Pirate Bay, but has sought the production of its poly-chronous Internet; a future where piracy is irrelevant. Further, innovations of P2P, such as BitTorrent, now underpin one of the most massive digital distribution networks on the Internet: Valve's Steam. Even the innovations of piracy promise to return to the system and routine and profitable modes of communication (Schiesel, 2004).

If escape is not the answer, then what other options might there be for dealing with transmissive control? The final chapter makes a shift from the theoretical discussions so far to policy matters related to transmissive control. Policymakers as much as pirates have attempted to respond to the issues raised by transmissive control. Usually their approach to the matter draws on concepts from Network Neutrality. Making transmissive control matter to policymakers offers a new set of challenges that help further elaboration the concept. What does the concept of transmissive control reveal? How does it re-conceptualize the Internet in contrast to Network Neutrality? What normative approaches does it offer that could lead to sound policy? Though some might argue that it would be better to end with a solid concept rather than muddle it with real world examples, this chapter raises important aspects of the theory of transmissive control specifically the ways or representing and understanding the operations of software that have been present throughout the dissertation. This chapter, in other words, offers some methods to study transmissive control that help those interested in the concept and those interested in policy. This chapter focuses on the approaches to traffic management software in Canada – a country whose ISPs have been leaders in using Deep Packet Inspection (Bendrath & Mueller, 2011; Mueller & Asghari, 2011).

The next chapter shifts to metaphors from the film *Stalker* as a way to discuss the conceptual shift from a story of struggle and elusion to a confrontation with the mysterious operations of transmissive control. *Stalker* is a film dealing with a mysterious environment known as the Zone. The film helps set the tone of the next chapter which seeks to reveal the operations of software. Where *Inception* helps explain asynchronicity, demon gives some terms to discuss the agency of software and *Moby-Dick* offers some pacing to the struggle to elude transmissive control, the film offers an atmospheric example for dealing with the often hidden operations of transmissive control. Like the characters of the film, policy-makers need a slow and deliberate pace to expose the operations of transmissive control. This choice of metaphor will become more clear as it develops throughout the next chapter.

Chapter Five: Making Traffic Public

Introduction

Gauze tied around a metal nut flickers through the air before naturally falling to the ground. A party of three travellers stand in an empty field and watch the trajectory of the nut. One among them, their guide, pays close attention to its descent. Any anomalies in its fall would be evidence of the hidden forces lurking in the field. The scene comes from the film *Stalker* by Andrei Tarkovsky. *Stalker* is a film about the journey of three men deep into a territory marked by an unspecified disaster known as the Zone. Their leader, a guide known as a Stalker, warns of the hidden dangers of the Zone to his party of a Writer and a Physicist. The metal nut is one instrument he uses to expose the anomalies of time and space scattered across the Zone. One of the deleted scenes of *Stalker* involved an anomaly of time looping endlessly. A loop of a tank column crossing a bridge would hint at the strange anomalous times of the Zone (Skakov, 2012, p. 141). Guidance by the Stalker avoids these dangerous mutations of time (or so he promises). Every few steps cause another nut to be thrown into the air. Slowly the party advances deeper into the Zone.

Where the last chapter focused on the flight away from transmissive control, this chapter seeks a means for the public to confront transmissive control. How might the lines and operations of transmissive control be rendered? More importantly, why attempt to elude transmissive control if escape provokes it more? Where resistance to transmissive control might be problematic, there still remains a need to respond to transmissive control and this might be done through policy and politics. Decisions about how to control the temporality of the Internet such as whether poly-chronicity is a desirable direction for the Internet requires some

political decisions. This final chapter then seeks to create methods to aid in the deliberation of transmissive control. It does not seek to resolve or answer the problem of transmissive control, but to work toward the conditions required to enable this deliberation. Though the concept of transmissive control stands on its own, the move to areas of policy and politics deliberately pushes the limits of concept.

This chapter uses the metaphor of *Stalker* because methods for confronting of transmissive control in politics and policy resembles the film's exploration of a mysterious environment. The goal is to develop methods of knowing the crystallizations of transmissive control. How is poly-chronicity expressed? What traffic is prioritized and what traffic is throttled? Unlike advocates of Network Neutrality, the concept of transmissive control does not assume an answer to the normative question of how to manage the asynchronicity of the Internet. The inception of the Internet certainly did not produce any consensus on the purpose of the network. Asynchronicity simply collapsed many different networks and their temporal economies into one without inter-network without actually formulating any response to tensions or conflicts. The tensions and lack of consensus allows systems of transmissive control to step in as an answer to the conflicts between temporal economies. Versions of a new poly-chronicity – a new Pandemonium – remain asymmetrical such that they will be continually resisted and ever more advanced.

Traffic management policies are like the anomalies of the Zone – usually unknown to those within them. Cycles of transmissive control pass in less than the blink of an eye. They pass in milliseconds once triggered. Exposing transmissive control – like how a camera might expose film – involves remembering the instant, recording the forces and effects during transmission of packets over networks. The public needs instruments to actively confront transmissive control just as the stalker uses the metal nut to reveal the forces of the Zone. To this end, this

chapter focuses on methods to record and remember the cycles of transmissive control. It discusses methods, technically known as Internet measurement tools, that would facilitate the public to record transmission from their home connection and pool these records as evidence of the effects of transmissive control. These methods could support a *public research project* where people would individually test their connections and pool their results into public records of the operation of transmissive control. These records would aid policy-makers in understanding and, in turn, responding to the challenges of transmissive control.

This chapter emphasizes the overall normative stance of the dissertation by advocating public research to study transmissive control. Its normative stance draws on the work of pragmatist John Dewey. He saw public research as both a necessity to study the issues affecting the public and that this research might allow the public to be informed of the issue. The methods discussed in this chapter have a similar goal. They seek to include the public in researching transmissive control and in this way inform the public about how it works. This is a precursor to moments of deliberation and debate. The software discussed in this chapter creates a memory that could support public deliberation. The approach differs from how policy-makers conventionally approach of transmissive control.

Transmissive Control and Internet Policy

Transmissive control has typically been represented as a problem of Network Neutrality in Canada. Since the perspectives have already been reviewed elsewhere (Powell & Cooper, 2011; Quail & Larabie, 2010; Stevenson & Clement, 2010; Stover, 2010; Wu & Yoo, 2007), this section will not duplicate an exhaustive overview; rather, it will only demarcate the approach from a transmissive control perspective. Network Neutrality, in general, advocates "all packets transmitted over the public Internet be treated equally, regardless of source, ownership, con-

tent or destination" (Longford, 2007: 13). The principle, advocates suggest, would prevent the discrimination of traffic (see Wu & Yoo, 2007). Underlying discrimination is a matter of the management of the control of a network. Who decides when Internet usage is out of control on the Internet and when to enact control online?

The 2009 CRTC hearings on Internet Traffic Management Practices has been seen as one of the major international inquires into matters of discrimination related to advanced traffic management software. The hearings began after the Canadian Association of Internet Providers (CAIP), an association of 55 small ISPs in Canada, submitted a complaint that Bell had begun throttling their wholesale connections (Anderson, 2008; Nowak, 2008b). Even though the CRTC denied CAIP's request to stop Bell from traffic management, they put forward a formal request for comments as part of formal hearings in 2009 (Geist, 2008b). The hearings brought together the major ISPs, small ISPs, Internet firms like Google and BitTorrent as well as numerous public sector organizations[21].

The last three chapters illustrate some of the strains on the representativeness for these hearings, particularly the ability of these hearings to represent software. Radical P2P hackers have become criminals. The Pirate Bay only have seats at their trial. Demons, on the other hand, have difficulty being represented by self-interested parties (cf. Latour, 2004). Consider the representation of BitTorrent during the ITMPs hearing. Rogers Communications spokesperson Ken Engelhart argued BitTorrent caused congestion as it "takes place 24 hours a day seven days a week at the maximum rate of speed that the customer's service permits" (Canadian Radio-television and Telecommunications Commission, 2009a). BitTorrent Inc. countered that "the average client is 'on' or active for 10-20% of the days of any given month"

[21] The CRTC maintains a public list of all filings by all participants of the hearings on its website. See: http://www.crtc.gc.ca/partvii/eng/2008/8646/c12_20081540o.htm.

according to the data they collect when a client "starts up or has been on/active for 24 hours" (BitTorrent Inc., 2009). Proper representation for BitTorrent would have aided a ruling since ITMPS typically target BitTorrent; yet, neither answer Rogers nor BitTorrent proved satisfactory since both parties had an invested interest when representing the software.

Proper representation of software has proven to be a problem well after the ITMP hearings ended. The CRTC eventually reached a decision to set forth a framework for ISPs using ITMPs. These practices could be used so long as ISPs were transparent about their usage and did not hamper innovation or reduce competition in Canada (Canadian Radio-television and Telecommunications Commission, 2009a). Prominent advocates of Network Neutrality, such as Michael Geist, Canada Research Chair of Internet and E-commerce Law at the University of Ottawa, and Milton Mueller, Internet governance scholar, cautiously embraced the framework (Bendrath & Mueller, 2011; Geist, 2009). Soon after the ruling, the lack of transparency hampered enforcement of the policy. Onus rested on the complainant to provide evidence of violations of these principles. Many firms have yet to comply and its even harder to make transparent their traffic management practices (Geist, 2011a). The Canadian Gamers Association, for example, found that Rogers Communication has been throttling *World of Warcraft* as mentioned in the introduction. Their complaints took nearly three years to be addressed by the CRTC (Ellis, 2011). More troubling they found that throttling occurred because Rogers "applies a technical ITMP to unidentified traffic using default peer-to-peer (P2P) ports" (Roseman, 2012). Throttling, in other words, occurred even to P2P traffic that Rogers had not justified – a violation of the CRTC guideline specifying that ITMPs "must be designed to address a defined need, and nothing more" (Canadian Radio-television and Telecommunications Commission, 2009a). Even though ISPs had agreed not to throttle without cause, evidence

proved otherwise. This case is just one of a thirty-six complaints about violations of ITMPs ruling documented by Geist (Geist, 2011a).

These violations illustrate the problem of software as a kind of forum shifting. Bell or Rogers sought to resolve tensions in the Internet by installing software in lieu of an actual political confrontation. ISPs avoid the accountability of public flora when encoding their solutions into traffic management algorithms. They may even be leveraging transmissive control to further their vertical integration as two of the complaints cited by Geist concern throttling P2P phone services, like Skype, that competed with the ISPs own telephony services. When found in violation, most times, firms have either to revise their public disclosure page or simply stop the practice. There is no retroactive accountability that would discourage ISPs from adopting traffic management policy. ISPs have the benefit of using a policy for a few years before they might be required to stop the practice. In this time, users change habits out of frustration, presumably the change in behaviour sought by ISPs in the first place.

While some violations might be deliberate, other violations – as Rogers Internet claims in the case of *World of Warcraft* – might be accidental. Rogers Internet claimed that their throttling of the game occurred due to a misconfiguration of their Cisco routers (Lasar, 2011). This very well might be the case as there is no real reason for an ISP to interfere with a popular game that would attract customers. Software misconfiguration further demonstrates the need for greater transparency of transmissive control as ISPs might simply make mistakes that effect Internet communication. Proper representation of the operations of software would detect mistakes before they cause major disruptions.

Oblique software processes are the main challenge to these issues of enforcement, compliance and error control. Software has less accountability because its operations never appear before Internet users. Transmissive control leaves no trace on its own as its operations occur

in the circuits of routers and switches deep in the Internet. A number of theories have approached the *invisibility* of software process. Richard Rogers (2004) refers to the difference as one between *front end* interfaces and *back end* software processes. Langlois (2011) argues that the web includes a number of semiotechnologies that she describes through Guattari's mixed semiotic framework. Though the web includes a number of *signifying semiologies*, information processes, such as the ones that define transmissive control, operate as *a-semiotic encodings* that "that work through the transformation of human input (meaningful content and behaviour) into information that can then be further channelled through other informational processes and transformed, for instance, into a value-added service" (2011, p. 22). Though Langlois's work on semiotechnologies extends beyond this section, it does point toward a tension between software routines and policy debates. Hence public deliberation will always be difficult without bringing greater transparency to the operation of their software. How can the operations of transmissive control be brought to the public light?

Early investigations into traffic management software offer a direction for the study of transmissive control that would aid policy matters. ISPs in the United States and Canada only admitted to traffic shaping practices after concerned media reform activists made these practices public. In 2007, the Electronic Frontier Foundation (EFF) and the Associated Press (AP) monitored BitTorrent traffic on the network of American ISP ComCast and detected it deliberately injected Reset packets into this traffic.[22] Deep Packet Injection, as they called it, disrupted BitTorrent communication by causing the computer on one end to think the machine on the other end had hung up. The practice allowed ComCast to diminish BitTorrent traffic on their network – another form of traffic shaping that creates tiers on the Internet. EFF discovered traffic shaping using a free software packet inspection tool. Their findings

[22] For a copy of the report, see: http://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

prompted an investigation by the United States Federal Communication Commission that eventually led to a ban on packet injection (Kravets, 2008).

Where the EFF and AP study focused on one ISP, the *Vuze* BitTorrent application sought to understand the impact of traffic shaping on Internet usage by asking its users to install a plug-in to monitor their traffic and send the results to Vuze for analysis. Eight thousand users responded and logged 100,000 hours of traffic usage data.[23] With this data, Vuze created a list of the Bad ISPs that throttled traffic. Many of the ISPs on the list had not widely publicized their traffic shaping, especially in Canada. The list ranked Canada's Cogeco as the second worst offender. This revelation spread through the news provoking public concern that fuelled the CRTC's hearings on ITMPs (Nowak, 2008a). In another example, IXMaps, a project of the New Transparency Project at the Faculty of Information at the University of Toronto seeks to identify how our information moves across the Internet and whether it passes through known points of government surveillance.[24] Concern over Internet surveillance arose after a leak revealed the National Security Association and AT&T partnered to install secret rooms in many of the major traffic aggregation hubs on the Internet. With the leak came the locations of some of the major surveillance hubs. IXMaps allows users to contribute their traffic routes to reveal whether a users' communication passes these sites or to potentially identify other sites. IXMAPs, in other words, reveals where surveillance might take place on the Internet (Clement, Paterson, & Phillips, 2010).

These examples, or so this chapter argues, provide insight into the interaction of transmissive control and policy – namely the development of public research methods to expose its operations and to aid in understanding the state of the Internet. Since transmissive control

[23] For details of the study and the methods, see: http://wiki.vuze.com/w/ISP_Network_Monitor.
[24] For more details about IXMAPS, see its website: http://www.ixmaps.ca/.

directly affects every Internet user, then their experiences become an idea mechanism to study its operation. A few research projects have sought to develop concepts and tools for public research such as crowdsourcing (Brabham, 2008a, 2008b; Brito, 2007; Howe, 2006) or citizen science (Hand, 2010; Irwin, 1995). They share a belief that "the Internet" as Bill Wasik writes, "is revolutionary in how it has democratized not just culture-making, but culture monitoring, giving individual creators a profusion of data with which to identify trends surrounding their own work and that of others" (2009, p. 14). Tools like IXMaps or Vuze illustrate the kinds of tools that could democratize monitoring of transmissive control.

Public research depend on John Dewey's notions of democratic deliberation and consensus. Science and Technology Studies have seized upon John Dewey's theory of publics to resuscitate the confrontation of technology as a moment of reflection and praxis (Callon, Lascoumes, & Barthe, 2009; Latour, 2005; Marres, 2010). Based on the work of Dewey, the following section argues that revealing transmissive control through public research is a precursor to an informed debate about the merits and problems of transmissive control. It would encourage as Darin Barney writes, "a thoroughgoing practice of citizenship will be one that also subjects the ethical commitment to technology *as a good way of life* to ongoing political judgement" (Barney, 2007, p. 38). Distributed methods could expose the acts of traffic management so it could be judged and contested. Many of the technologies driving concerns about network management in Canada, including Deep Packet Inspection, raise important questions about how to manage scarce bandwidth in support of the public good. For example, the First Nation ISP, K-Net, uses traffic shaping to prioritize its community video-conferencing over other traffic (McIver Jr., 2010). Formulating a similar sense of public good priorities on the wider the Internet will prove challenging, but a better representation of software would support the CRTC hearings debating traffic management. Even further, it could dis-

cuss in public spheres where Internet users could formulate a response to transmissive control (Downey & Fenton, 2003; Fraser, 1992) or even foster political antagonisms akin to a social movement that might seek to diminish or sense the legitimacy of ISPs to make decisions about their traffic management (Angus, 2001). These places of deliberation might eventually find an effective solution to the problem of the Internet's inception.

Similar to how the stalkers of the Zone engaged in their own public research, this section has argued for more public engagement in Internet research. Proper deliberation on transmissive control requires an awareness of software easily made possible by enlisting people to study their Internet connections. As the CRTC's ITMP hearings have shown, the algorithms of the Internet need more attention. Public research offers one method to study transmissive control. The following section develops this concept through a discussion of the foundational work of John Dewey on publics and democratic methods. Part of this explanation of Dewey will contrast his work with his one of leading critics, Walter Lippmann, in order to draw out how public research depends on a different set of assumptions about knowledge. It explains how Dewey offers a more robust and participatory theory of knowledge than Lippmann and that this theory of knowledge aligns with the problem of confronting control.

Why Public Research as an Answer to Control?

Military checkpoints blocks the entry into the Zone. Signs warn the public to stay clear of the Zone. Some do not obey the sign and they are known as stalkers. These people, like the guide of the film, explore and study the mysteries of the Zone without the government's consent. These nomads have their own sciences: metal nuts and habitual paths explore the anomalies of the Zone. This chapter has an affection for these stalkers as they exemplify the kind of public research needed to study transmissive control. Their confrontation with their environ-

ment speaks to a matter of recognition, of becoming aware of the Zone. How might a similar journey of discovery cultivate a better awareness of the Zone? Public research, like the kind John Dewey advocated and like the very journey of these amateurs into the Zone, is an important democratic practice – one capable of confronting the hidden operations of transmissive control.

The concept of the public arises from John Dewey and his pragmatic political theory. A public is a group of persons that results from an event or phenomena. Dewey defines the public as "all those who are affected by the indirect consequences of transactions to such an extent that it is deemed necessary to have those consequences systematically cared for" (1927, pp. 15–16). Publics would be those persons affected by new legislation or even environmental disaster. Indirect consequences in the case of the Internet refer to those persons who have their communications throttled or find their access over their monthly limit. Marres (2004, 2005, 2010) in her ongoing re-appraisal of John Dewey emphasizes that "publics are called into being by *issues*" [emphasis added] (2005, p. 209). Issues, a sort of political catch-all for Marres that replaces Dewey's term *transactions*, draw people into public life. Public participation does not occur without *issues*, such as transmissive control. At the moment of invocation, a public can develop into a tangible political force capable of "systematically car[ing] for" their provoking issue.

Behind the work of Dewey is the belief that publics are an "immense intelligence" (1954, p. 219) since political transactions directly affect them. As he writes, "the man who wears the shoes knows best that it pinches and where it pinches, even if the shoemaker is the best judge of how the trouble is to be remedied" (1927, p. 207). This insight also applies to the study of transmissive control as Internet users are the best to understand its effects. Innovative methods in communication and collective research would allow for a kind of experimental social

inquiry necessary for democracy. Understanding Dewey's approach to knowledge and social inquiry, however, depends on situating Dewey in the context of other democratic thought, specifically his contemporary Walter Lippmann.

The argument that publics possessed intelligence was, in part, a response to the pessimism of his peer Walter Lippmann who questions the capacities of the public. Where Dewey embraces publics as a vital actor of democracy, Lippmann shuffles them into the audience. People never have the time nor the attention to understand and process the events of the day. Democratic theory too often depends on an *omnipotent citizen* capable of learning and processing volume of information daily (1922, pp. 180–181). A realistic vision of democracy, to Lippmann, requires a government or media that functioned as a group of insiders to watch the world and present an observable reality to its citizenry. The purpose of what-Lippmann-calls intelligence work "is not to burden every citizen with expert opinions on all questions, but to push that burden away from him towards a responsible administrator" (1922, p. 251). Intelligence works consolidated the instruments of knowledge collection, assigning it to a scientific administration similar to the approach of the government of the Zone or even the CRTC. His critique resonates with a common refrain in studies of democracy and technology where technical issues cannot be understood and judged by the public. Volumes of necessary information or knowledge impede the citizen for accurately perceiving technology and judging it (see Barney, 2007).

Lippmann's solution clearly manifests in the Canadian Radio-Telecommunications Commission's approach to Internet regulation. Policy experts and lawyers convene in their chambers in Gatineau where expert opinions and insider knowledge portray the state of the Canadian Internet. Inviting the public to consult at times and not inviting the public in other circumstances (see Wynne, 2007). For example, when the CRTC sought to investigation into

Internet broadcasting, they labelled it a fact-finding mission – a category of inquiry that did not have the same onus for public participation as a formal hearing (Geist, 2011b). These examples illustrate that public participation is always conditional on the part of the CRTC. These instruments favour the tendencies of experts and CRTC directors who have been trained to use these instruments.

Public hearings not only treat the public as adjunct, but also treat knowledge about the Internet as pre-existing the inquiry. It already exists and it simply needs to be presented in order to understand the state of the Internet. Such knowledge is not readily available and in most cases, has to be created by projects like IXMaps and Vuze. The public, even though they are affected by product of control, do not have a way to translate their experiences into research that could inform policy or more accurately the public can only vocalize its knowledge through the legal instruments of the hearing. Dewey did acknowledge expert decision-making in contemporary democracy. Institutions, such as the CRTC, were incremental solutions in the ongoing of development of democracy (1927, pp. 123–124); new ways of knowledge would eventually replace them. The legal approach to knowledge differs from the more experimental question for knowledge advocated by Dewey. He argues that knowledge and understanding is a process – an expression maybe – that changes and develops through research.

Lippmann, however, suffers from a circumscribed *spectator theory of knowledge* (see Ezrahi, 1999). Lippmann's shortcomings (and by extension all those who seek to shield the public from research) can be explained through his concept of a *pseudo-environment*. It designates the pictures in a person's head through which they interact with their environment. Since the citizen cannot *see* the complex global politics, they cannot form an appropriate pseudo-environment necessary for informed decision-making. Watching and spectatorship underlie Lippmann's way to knowledge since citizens observe and compose opinions based on these

observations. For example, "the analyst of public opinion must begin then," Lippmann writes, "by recognizing the relationship between the scene of action, the human picture of the scene and the human response to that picture working itself out upon that scene of action" (1922, p. 11). Lippmann problematically conflates the ways to knowledge with perception. If knowledge is only seen through "pictures in peoples' heads" then the limits to attention prevent the democratic citizen from full participation. Knowledge for Lippmann results from an already constituted reality for experts to observe.

Dewey, on the other hand, sees knowledge as a process developed through experience not spectatorship. As Ezrahi writes "seeing is always an aspect of acting and interacting, of coping with problems and trying to adapt an improve, rather than just contemplate, mirror or record" (1999, p. 322). Spectatorship imposes an unnecessary distinction between reality and the knowledge of reality[25]. Dewey resolves this problem by considering the public as participant not a spectator. As he writes "if we see that knowing is not the act of an outside spectator but of a participator inside the natural and social scene, then the true object of knowledge resides in the consequences of directed action" (Dewey quoted in Ezrahi, 1999, p. 318). An inversion takes place within this quote where the public no longer receives information, but produces information. Knowledge results from experience and process not just witnessing and spectacle. His way to knowledge resonates with the approaches of Vuze and the EFF who created knowledge through experimental methods.

Democratic society needs to developed experiential learning in contrast to spectatorship according to Dewey. "Democratic ends", as Dewey recognizes in the title of a message sent to the first meeting of the Committee for Cultural Freedom in 1939, "demand democratic methods for their realization" (1990, pp. 367–268). As he writes in that same speech, "an American

[25] Latour refers to the disembodied observer as the problem of a mind-in-a-vat (1999, pp. 16–17)

democracy can serve the world only as it demonstrates in the conduct of its own life the efficacy of plural, partial and experimental methods in securing and maintaining an ever-increasing release of the powers of human nature, in service of a freedom which is cooperative and a cooperation which is voluntary". Dewey's political writings argue the necessity of an experimental way to knowledge and sought to create the conditions of literacy to foster democratic methods of knowledge collection.

The challenge of democratic methods resonates with the work of Callon, Lascoumes and Barthe (2009) who build upon Dewey's sense of knowledge production through their concept of a *common world*. The term signifies the results of a collective process of understanding whereby a new sense of the world unfolds. Building a common world involves a sense of reality that grows to better include its participants. They use the word composition when discussing the process behind common worlds. It implies that "the uncertainties of groupings that simultaneously define (or redefine) the significant entities" (Callon et al., 2009, p. 132). New common world results out of c*ontroversies* another term in their nomenclature that functions similarly to *issues* for Marres. These moments of becoming "enrich democracy" and "are powerful apparatuses for exploring and learning about possible worlds" (2009, p. 28). Controversies are moments for composition such that "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" (2009, p. 32). Robustness here is a trait of the composition of a common world that refers to how it integrates different actors and questions. How does it inform or enhance its constituents? Their work, rich with a sense of the complexities of democracy in a technical age, finds a possibility in those affected and, in this way, offers a direction for the study of control. The quest is for the public to research the Internet and to compose a common world that includes the operations of transmissive control.

At this point, the normative dimensions of this dissertation and this chapter should be clear. Issues or controversies like Network Neutrality are not simply matters to be resolved, but opportunities of building a common world. Public research, far from just generating data, cultivates a public capable of understanding and composing itself in relation to the demons and lines of the Internet. Precisely because public research enlists the public, it is the ideal means to confront transmissive control. The next challenge is to find the necessary democratic methods to expose control. The following section introduces the concept of *software mediators* as the necessary instruments for a public research into control.

What Mediators for Transmissive Control?

The dangers of the Zone elude human perception. Throughout the film, the Writer and the Physicist argue with the Stalker whether the Zone actually is a threat. The Physicist confronts the Stalker and questions his faith. The same fears taunt the characters in the film *Stalker* who never fully believe in the power of the Zone. In response, the Stalker improvises methods to detect anomalies in the Zone such as the metal nut. No doubt many such devices exist in the Zone. All these tools provide a means for guides to study and understand their environment. They are, in short, democratic methods that aid in understanding the Zone. The question remains what instruments would expose transmissive control? The task is not unlike Deleuze's suggestion for the Left. He writes,

> For the Left, this means a new way of talking. It's about not so much a matter of winning arguments as of being open about things. Being open is setting out the 'facts,' not only of a situation but of a problem. Making visible things that would otherwise remain hidden. (Deleuze, 1995b, p. 127)

Note his use of making – or in the original French <<*rendre*>> which means to render, to make or to return – visible, as opposed to finding or revealing (cf. Latham, 2010). His quote come from a "political digression" that the left needs mediators – the concept put forward in the larger article – that refers to the ways of resonances. Language mediates Deleuze's self-expression, just as people might mediate between disciplines (1995b, p. 125). Public research requires mediators that compose the instant activity of transmissive control into a common world.

The following section introduces two software mediators, NDT and Glasnost, to explore how they might aid in the composition of a common world. Engineers and software developers have also developed tools to test and repair their networks. These kinds of mediators – software mediators – offer another way into understanding the Internet. There has been a near constant drive to develop these mediators commonly called Internet measurement tools in the technical literature since the advent of packet switching (Cerf, 1991; Molyneux & Williams, 1999, pp. 292–294). A literature has slowly developed to evaluate these different tools (Bauer, Clark, & Lehr, 2010; Dischinger et al., 2010; Dischinger, Haeberlen, Gummadi, & Saroiu, 2007; Dovrolis, Gummadi, Kuzmanovic, & Meinrath, 2010; Kreibich, Weaver, Nechaev, & Paxson, 2010; Paxson, 1999; Prasad, Dovrolis, Murray, & Claffy, 2003). This section will not attempt to exhaustively document all Internet measurement tools; rather, a few examples explain the relationship between software mediators and transmissive control. These examples have been drawn from the Measurement Lab project that will become more significant as this chapter moves to a discussion to implementing a larger public research project in Canada.

Before introducing these software mediators, they should be distinguished from conventional methods of understanding performance of the Internet. Many indicators exist throughout the world to explain Internet usage but different methods are used to produce them. The

Organization for Economic Cooperation and Development (OECD), for example, surveys its member governments to compare their national average advertised download speeds and the types of usage limits on monthly plans.[26] The Canadian Internet Use Survey 2009 surveyed 23,000 Canadians. Results showed that email remains the most popular application among this group.[27] Software mediators compliment these types of research projects, but also seek to go further by enlisting the public in the project itself.

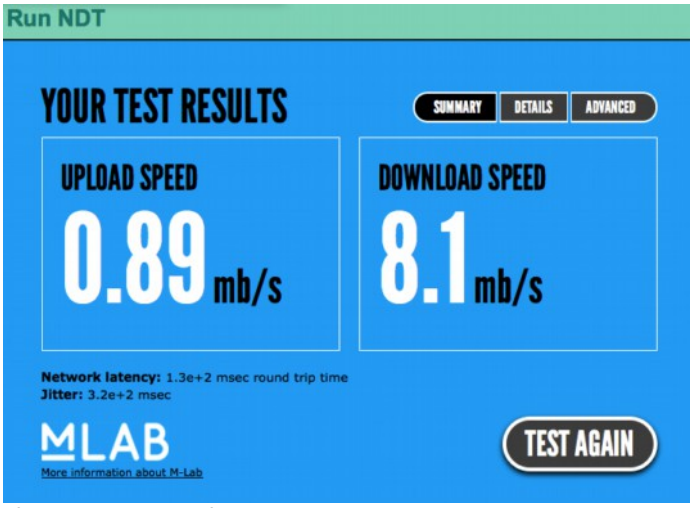


Figure 24: NDT Results

The Network Diagnostic Tool (NDT) is the first software mediator to be considered. The tool measures the maximum bandwidth capacity for downloading and uploading. In addition to running measures of the capacity, the test also measures for latency or delay to receive requested information and jitter (or the regularity of packet delivery times) seen in Figure 24. These measures were discussed in Chapter Three and Chapter Four as potential techniques to manage the rate of transmission. The test works by sending and receiving as much data as possible during a ten second window. Data transferred provides an upload and download

[26] The OECD's webpage for a complete list of their measures, see: http://www.oecd.org/document/54/0,3343,en_2649_34225_38690102_1_1_1_1,00.html.

[27] For the StatsCan News Release summarizes the project, see: http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-eng.htm.

capacity, but the tool also collects detailed logs to calculate jitter, latency and congestion (Bauer et al., 2010, p. 31). Aggregating data collected from NDT produces overviews of Internet patterns over time and space. Each NDT test logs the location of the tester as well as the time and date. When analyzed the results illustrate trends in rates of transmission.

The examples below illustrate the capacity of NDT to chart the systematic aspects of transmissive control. Figure 25 charts the download speeds for major Canadian ISPs over time.

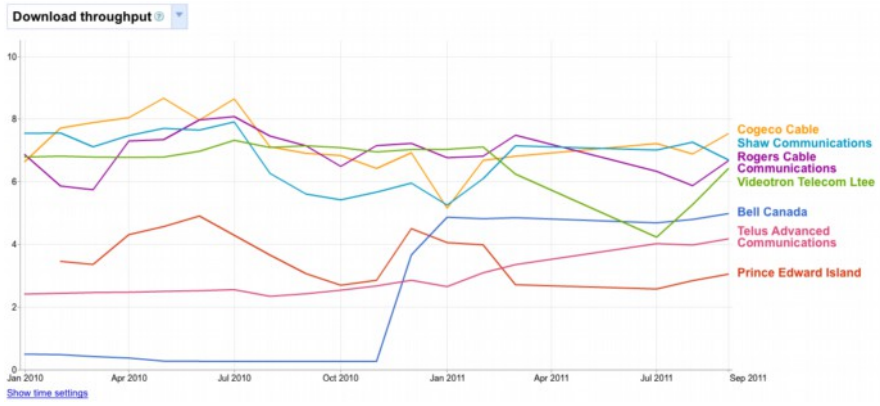


Figure 25: Download Rates by Province

NDT data might be used to compare Canadian provinces like ISPs. Figure 26 maps NDT congestion data in Canada. Circles overlaid over province illustrate their respective levels of congestions. Circles vary in size according to the number of tests conducted in a province (larger indicating more tests) and vary in colour to illustrate rates of congestion from low/blue to high/red. Though not possible to represent, the visualizations plays *over time* to congestion trends year over year. This chart would support or dispute claims about the level of bandwidth scarcity often used to justify greater traffic management.

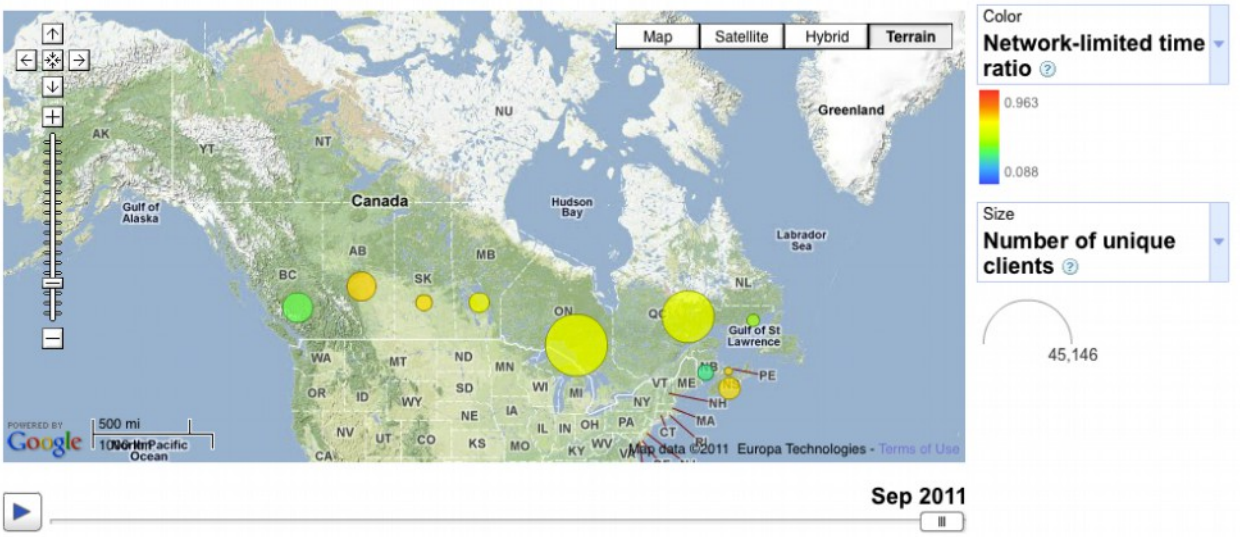


Figure 26: Congestion by Province

The results offer a sense of how much congestions exists in different provinces of Canada. Ontario appears to have more congestion that British Columbia. This type of data could be used to compare the success of different provincial or even municipal broadband development policies, such as the Alberta SuperNet or Fredericton's Fred-eZone (see Middleton, 2007, pp. 17–18). Data might also illustrate other digital divides beyond just access to the Internet where users can get online but suffer from degraded connectivity due to congestion.

Even though NDT offers a way to understand the baseline of the Internet's capacity, it does not satisfy many of the questions raised by transmissive control. Its data only illustrate the max capacity of different networks not how different rates of transmission participate in a temporal economy. The question is not simply about the base capacity, but whether some applications have different rates of transmission on the same connection. Another tool, known as Glasnost, offers a different approach that exposes different in the transmission rates of applications.

Glasnost is another mediator that seeking to reveal traffic management on different applications – one of the most overt usages of transmissive control. It works by simulating the traffic flows for a few different types of applications and comparing these transmission rates with a control flow.

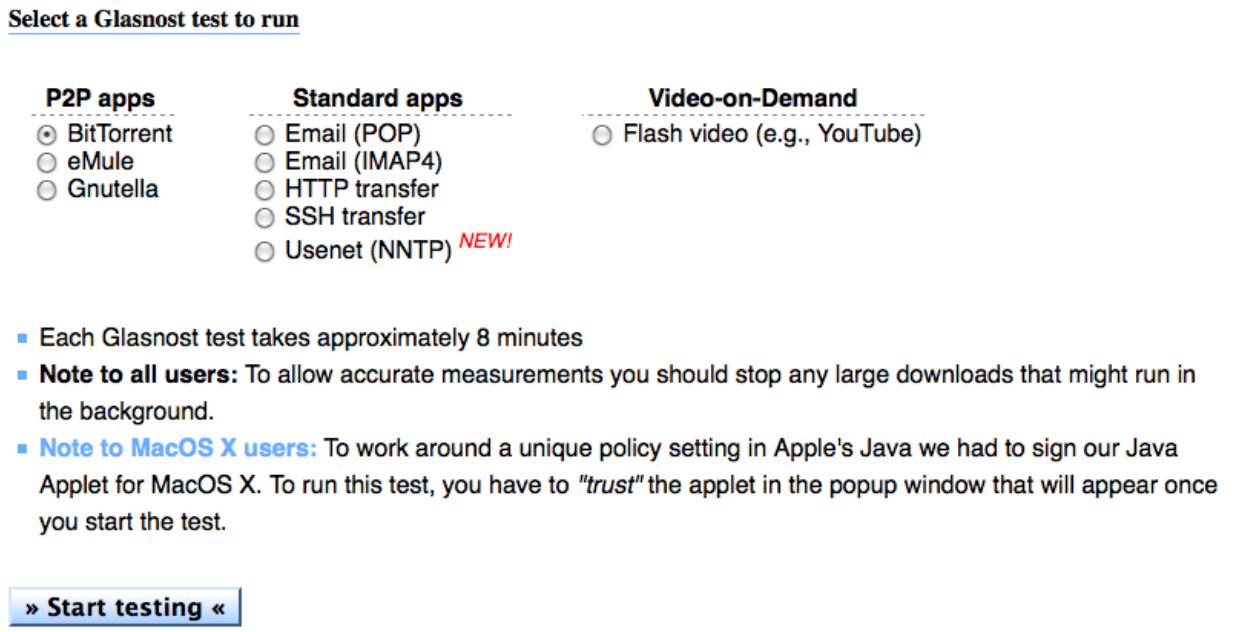


Figure 27: Starting a Glasnost Test

If a simulated flow has a very different rate of transmission than the control flow, Glasnost considers the difference as evidence of a traffic management policy. Figure 27 depicts the tests offered by Glasnost. Users have an option to choose one of nine protocols such as BitTorrent, Gnutella, Usenet and Flash video then launches a Java applet that displays a simple progress bar as it runs the 8-minute test. Behind the progress bar, the Java applet is running a series of test over TCP to the testing server. Each time it sends two traffic flows to the server: one comprised of BitTorrent packets and the other comprised of random control packets. It determines the presence of traffic shaping based on the variance in rate of control traffic and the Bit-

Torrent traffic. Not all differences occur due to traffic shaping. Sometimes the *best efforts* routing simply causes differences (demonic feuds perhaps) so Glasnost sets certain thresholds of variance as indicative of shaping. A link on the page offers more details about the test such as the whether the tool detected the presence of any traffic shaping (Asghari, Mueller, van Eeten, & Wang, 2012; Dischinger et al., 2010).

Though the project does not use the concept of transmissive control, Glasnost directly probes questions of transmissive control by investigating the different rates of transmission for various kinds of applications. Results could show how an ISP or network connection prioritizes one application over another, e.g. does BitTorrent take more time than Flash video? Does email – a more conventional application – outperform a P2P application like Gnutella? Although no study yet exists, Glasnost could be used to compare the relations of transmission between different applications over time. It could reveal how a poly-chronous temporal economy might be crystallizing on the Internet over time. Conducting such a project would require much more tests and resources, a problem that will be discussed later in this chapter.

The *Network is Aware* project at Syracuse University led by Milton Mueller (2002, 2010) has been the most active in analyzing the results of Glasnost. They have processed the raw Glasnost results to generate statistics about the usage and development of BitTorrent traffic shaping. Interestingly, the project has spent a considerable time translating Glasnost's logs into usable data due to differences in the design principles of Computer Science and the Social Sciences. Computer Scientists prefers raw or unedited logs requiring considerable computation to become aggregated data for conventional social science analysis. Their difficulties, as they admit themselves, are common among public Internet researchers and a clear answer does not exist (Asghari et al., 2012). After all this data processing, the project has been able to chart the changes in the shaping of BitTorrent.

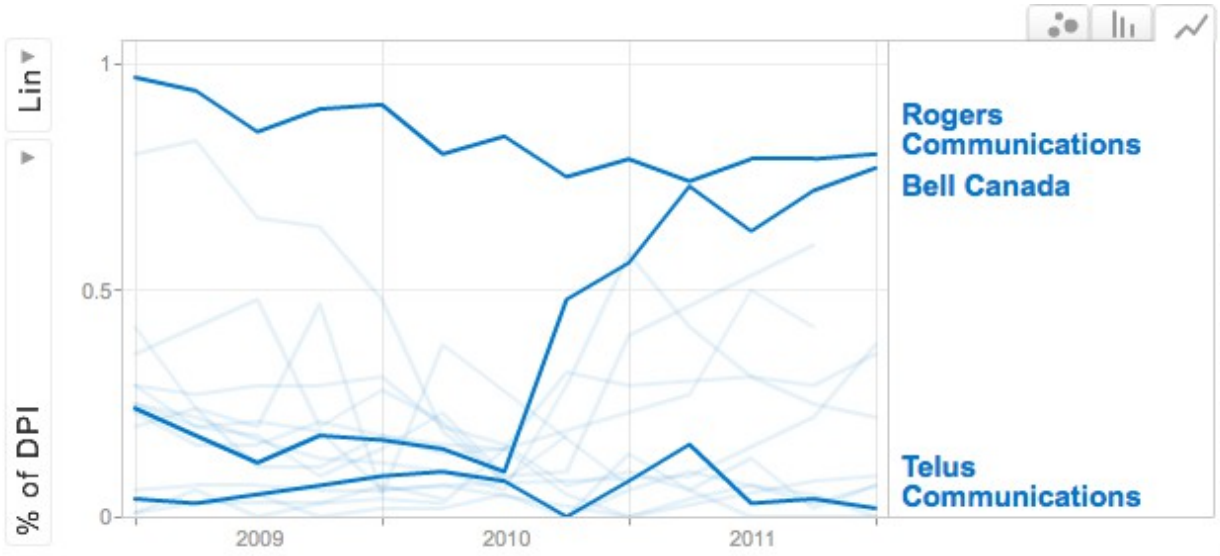


Figure 28: Canadian Glasnost Results for Canada from 2009-2012

Figure 28 illustrates the kind of results projected by the *Network is Aware* Project. The chart comes from their results page.[28] The left axis of the chart depicts the percentage of Glasnost tests detecting evidence of traffic shaping where the bottom axis depict time. Three of the major ISPs have been included in the chart to show how Glasnost test records changes in traffic management policies and by extension transmissive control. CRTC hearings confirm some of Glasnost results as Rogers Communications openly admitted to throttling BitTorrent Traffic in the 2009 hearings on Internet Traffic Management Practices and test results indicate that well above 50% of tests on Rogers detected traffic shaping. Telus, on the other hand, confirmed they did not employ such measures. Test results for Telus did not detect traffic shaping when controlling for false positives (Canadian Radio-television and Telecommunications Commission, 2009a). Bell Canada complicates this analysis as they seemingly only started to shape traffic after 2010 even though they had been widely reported to be traffic shaping since 2008 (Kapica, 2008). Perhaps errors in the Glasnost code caused the errors or low tests num-

[28] For the rest of the results, see: http://dpi.ischool.syr.edu/countries.html.

bers in Canada prevent more accurate results. Whatever the case, these results indicate at least the possibility of these tools to expose transmissive control through public research.

What do these mediators do in effect? What are the characteristics of their common world? How do they expose transmissive control? These tests measure a moment of the network-becoming capturing aspects of its expression including the rate of communication between nodes as well as evidence of overt traffic shaping. Moments would become an inaccessible past without the logs from these tests. Logs constitute a memory of Internet transmission. These logs allow for interpretation and study allowing for a sense of the patterns of transmissive control and its trends. Even if respective ISPs released their trends, it would be a tremendous project to assemble a collective record. Remembering the instantaneous operations of traffic management requires software mediators to translate software processes into enduring records. These software mediators illustrate how publics might confront transmissive control. NDT and Glasnost record the operations of the network and these recordings become a kind of memory for the instant effects of transmissive control. With these tools in mind, the next section seeks to unite software mediators with publics through a return to the questions of time indicative of transmissive control.

Mediators, Memories and Publics

Software mediators allow for the composition of a common world with a common memory. The task resembles the work of stalkers in the Zone. Through their travels in the Zone, stalkers map its territories and plot the invisible dangers similar to how the stalker of Tarkovsky's film follows a specific path further into the Zone. His knowledge from the Zone comes from his experiences in the Zone – his own experimental journey. The Stalker also refers to his mentor, nicknamed Porcupine, who introduced him to the Zone and let him on his early

expeditions. Since the military prohibits access to the Zone, their experiences become their only sources of information about its features and threats. Their travels are a kind of do-it-yourself science that maps anomalies of their respective Zones. They gradually build a common sense of the Zone from their individual experience. While stalkers might face anomalies and soldiers, publics and software mediators face another kind of challenge.

The challenge is that transmissive control operates in a fragmented, opaque way that Deleuze describes as *dividuality*. He writes, "we no longer find ourselves dealing with the mass/individual pair. Individuals have become 'dividuals,' and masses, samples, data, markets or 'banks'" (1992, p. 5). They dissolve into a variety of profiles and data types. People become affected by transmissive control when software recognizes their Internet communications according to a central pattern encoded in network memory banks and algorithms. A user might have some of their traffic throttled, other traffic experiences acceleration. These experiences appear unique or individual, a product of targeting and redlining. Dividuality increases differences and fragmentation as it dissects users and stitches together dividuals. Publics are ever thus dissected and re-assembled into new collections. Deseriis (2011) expresses this condition well in the following passage,

> by breaking down the continuity of the social bios into dividual sessions and transactions, the engineer of control produces what Franco Berardi (2009) calls a "cellularized" info- time, an abstract time that is no longer attached to the body of any specific individual but generated by the automated recombination of dividual fragments of time in the network. (p. 392)

Deseriis suggests the "social bios" becomes "dividual sessions and transactions". Different rates of transmission for different applications create multiple publics, even creating antagonisms between these publics as network administrators pits piratical bandwidth hogs against

profitable value-added services. Since these assignments do not leave a trace by default, moments of reflection evaporate without a trace. Software mediators and publics must compose a commonness amidst the dividual moments of continuous control.

Transmissive control does produce a common *computational memory*. Memory is an important process of aggregation in systems of control. Packet by packet, flow by flow, algorithms find patterns and build models. They use these findings to manage communications dynamically. Profiles function to produce dividuality through a kind of mechanical remembrance. In this way, transmissive control encodes flows of traffic as aggregate profiles or dividualities and then assigns them based on pattern recognition in Deep Packet Inspection. Dividuality depends on an automated remembering. Yet, the commonalities of dividuality and control reside on servers opaque and publicly inaccessible. Linkages between dividuals simply cannot be read and understood. Unforeseen commonalities also result from the complexities of traffic management policies and the unpredictability of code. Publics and software mediators must translate this computational memory or past into a common memory. Composing a public memory would draw in the recordings from software mediators – the instances of dividuality – to compose common memory; it isan act of remembering of Internet.

Software mediators offer a means to translate this computational memory into some new temporalities of research and public deliberation. The purpose of a common memory would be for reflection and exploration; one indication of a common world and a public. This memory may, at first, seems similar to the plea for time made by Harold Innis. The "glorification of the life of the moment", as Innis states during a critique of Henri Bergson, is a problem of too much emphasis on the moment that hinder a reflection of the timeless questions (1951, p. 89). Though Innis points toward the need to question contemporary temporalities, his

emphasis on the eternal leads to a plea uninterested in current political questions regarding technology (see Carey, 1989, pp. 105,109–132). Though the pleas of Innis should not be ignored, Sheldon Wolin (1997) offers a better sense of the production of a time to reflect and deliberate. Political time, he argues

> requires an element of leisure, not in the sense of a leisure class (which is the form in which the ancient writers conceived it), but in the sense, say, of a leisurely pace. This is owing to the needs of political action to be preceded by deliberation and deliberation, as its 'deliberate' part suggests, takes time because, typically, it occurs in a setting of competing or conflicting but legitimate considerations. Political time is conditioned by the presence of differences and the attempt to negotiate them. (np.)

In order for democratic societies to function, they require a time for deliberation and negotiation which, in the case of the Internet, concerns the management of finite bandwidth between many temporalities. Importantly, political time requires preservation of "preserving bodies, goods, souls, practices and circumscribed ways of life" as Wolin writes, but also a preservation of the acts of traffic shaping that might illustrate the kinds of decisions made in the deployment of transmissive control. The problem is that "in contrast to political time, the temporalities of economy and popular culture are dictated by innovation, change and replacement through obsolescence. Accordingly, time is not governed by the needs of deliberation but by those of rapid turnover". The challenge is to become aware of control, so that it might be deliberated in political time.

A political temporality, however, is not simply a *slow time*. Connelly (2002) offers one of the most extended discussions of this challenge, one that extends the questions of Wolin. A new political temporality does not simply involve a slow time as "a slow, homogeneous world often supports undemocratic hierarchy because it irons out discrepancies of experience" (Connelly,

2002, p. 143). The challenge, he writes, "is not how to slow the world down, but how to work with and against a world moving faster than heretofore promote a positive ethos of pluralism" (p. 142). A political temporality might develop an awareness of the multiplicity of times on the Internet, perhaps even to support their proliferation and interoperation. Such an awareness needs to be approached with caution since a multiplication of temporalities mirrors strategies of dividuality. A political temporality could also fragment and tier the commonness of the public. Given these concerns, the composition of a public memory also offers new compositions with computers and publics, Computer Science and Social Sciences to come to new collective understandings of the world.

How to merge publics and software mediators into a public research project? The major challenge with any of these software mediators is that they require an infrastructure for their operation and for their results to compose into a public memory. To this end, the dissertation has developed and submitted a plan to create a broadband testing infrastructure. Based on a survey of the field to be discussed, this chapter argues that the Canadian Internet Registration Authority (CIRA) would be able to establish an infrastructure for public broadband testing infrastructure in Canada based on the standards from the Measurement Lab Initiatives. These findings were submitted to CIRA for review. As of July 2012, CIRA has committed to implementing this vision.

Toward a Large-Scale Public Memory: M-Lab in Canada

What organization would be interested in such a project? Giacomello and Picci cite six different organizations producing data about the Internet: international organizations (the United Nations and the Organization for Economic Cooperation Development), national statistical offices and other government entities (the United States Census Bureau), academic research

institutions (the Center for Communication at University of California Los Angeles and The Cooperative Association for Internet Data Analysis), Internet bodies (Internet Engineering Task Force and Regional Internet registries), pollsters and other private organizations (2003, pp. 374–380).

Internationally, these organizations have been involved with different Internet measurement options. The European Union has partnered with SamKnows and has begun an international broadband testing initiative. The Federal Communications Commission in the United States is perhaps the most active government entity in the area. It has collaborated with all major testing tools as well as launching its own national map of broadband speeds and prices since 2010 (I. Paul, 2010). In Greece, the Hellenic Telecommunications and Post Commission with Greek Research and Technology Network (GRNET SA) partnered with the M-Lab for broadband testing in August 2009 (Albanesius, 2009). Academic institutions have played a major role in developing tools such as components of M-Lab and the Netalyzr tool (Dovrolis et al., 2010; Kreibich et al., 2010); however, they have not launched programs as expansive as government bodies. In addition to GRENET SA, an academic research network, working with M-Lab, the Australia's Academic and Research Network (AARNet) also partnered with M-Lab in June 2010 to offer testing servers in the South Pacific region (Australia's Academic and Research Network, 2010). Internet bodies in Sweden, further, have been highly active in broadband testing. The Swedish register Stiftelsen för Internetinfrastruktur (.SE) has run their own public testing infrastructure based on a modified version of SpeedTest since 2006. Their project, Broadband Check <<*Bredbandskollen*>>, measures both fixed and wireless Internet connections, attracting a major user base of mobile testers. Its 15 million end-users have conducted 50 million measurements since its launch (The Internet Infrastructure Foundation, 2010). Private firms have been much more active in broadband measurement.

Many vendors of traffic management software leverage their install base to report trends of Internet usage. Notably, Cisco[29], Sandvine[30] and iPoque[31] release reports on Internet trends based on the statistical components of their traffic management software.

Have any of these kinds of organizations been active in Canada? Certainly, Canada has the necessary institutions to launch a public research project. These institutions include the regulator the CRTC, advocacy groups like Open Media, academic network research groups such as Canada's Advanced Research and Innovation Network (CANARIE) or Ontario Research and Innovation Optical Network (ORION) and the national registrar Canadian Internet Registry Authority (CIRA). Unfortunately, none of these organizations has to date launched a project. Most Canadian ISPs, specifically Bell[32], Rogers[33], Cogeco[34], Shaw Internet[35], Primus[36], Sasktel[37] and Videotron[38], all host their own versions of SpeedTest. The CRTC may be partnering with the SamKnows, but nothing has confirmed on matter other than a speech by Leonard Katz, then-Acting Chairman, at the 2012 Canadian Telecom Summit (Katz, 2012). OpenMedia, a leading Internet advocacy group in Canada, has supported the idea of greater transparency of broadband and continues to explore opportunities.

---

29 An example can be found here: http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html.

30 Sandvice releases quartery reports on their broadband trends here: http://www.sandvine.com/news/global_broadband_trends.asp.

31 Ipoque has launced an Internet Observatory and their reports may be found at: http://www.ipoque.com/en/news-events/press-center/press-releases/2011/ipoque-launches-Internet-observatory.

32 The test can be found at: http://206.47.199.107/.

33 Found at: http://www.rogers.com/web/Rogers.portal?_nfpb=trueand_pageLabel=support_InternetServices_speedCheck.

34 Available at: http://speedtest.cogeco.net

35 Available at: http://speedtest.shaw.ca

36 Available at: http://speedtest.primus.ca

37 Found at: http://www.sasktel.com/Internet/speedtest/index.html

38 The test is available at: http://testvitesse.videotron.ca/index-en.html

Of all these organizations, this chapter focuses on developing a national broadband testing infrastructure with CIRA. A fit appears between the objectives of CIRA and a public research project. In line with its corporate vision, the CIRA seeks to foster greater transparency about the Internet for its stakeholders. To address these concerns, CIRA wishes to develop a national public broadband testing tool to study the state of the Canadian Internet. If CIRA is interested, the next step would be to outline how CIRA could build a national public broadband testing tool to study the state of the Canadian Internet. The task involves deciding on the most appropriate broadband testing tools and developing a deployment strategy, i.e. where to build servers? How many servers? CIRA would have to build an infrastructure to support web-based software tools that allow residential users to probe their connection to the Internet through measurements, such as NDT and Glasnost. In doing so, CIRA would be the first institution in Canada to launch and promote a robust public broadband testing initiative.

Any project to succeed in creating a public memory must always keep in mind the values of public research articulated by Dewey. The following four principles translates the values of public research into more formal guidelines applicable to developing a national infrastructure. These values were included at the start of the report submitted to CIRA:

1. *Any solution to broadband measurement must be a working solution*. Home users should be able to easily test their home connection and learn about the results. Data received should also be interesting to researchers, companies and academics. The foundation of any testing solution, then, is working tests producing data that helps policy-makers, businesses and citizens make informed decisions about the Internet in Canada.
2. *CIRA must ensure a public broadband testing solution is open and transparent.* An evaluation must consider both the openness of both its methods and data. How does a tool

allow for scrutiny of its methods? Is its code open source or its methods documented in public? Further, how is the data available to the public? Are results available in raw data? Are aggregated logs available? Who has access to data? An open license might simply be in the public domain or a more restricted license only for non-commercial usage. An evaluation must consider how tools open their methods and release their results.

3. *Any solution must be adaptive by allowing for new tests that answer new questions posed by a changing Internet*. The Internet is continually changing and any tool needs to have a strategy to adapt to this dynamic infrastructure. How does a testing solution accommodate new research questions or changes in the Internet? Further, if people do contribute by developing new tests, how does a testing solution accommodate their contributions? The challenge, in short, is to future-proof the test and to ensure venues for public participation.
4. *Any proposal must include means to ensure that the public actually engages with it.* A working testing infrastructure depends on public participation. CIRA should find a tool that realizes that home users have the best perspective to conduct research about the Internet since they are the most affected by its conditions. Their participation is a vital component of understanding the state of the Canadian Internet. With this emphasis on participation comes a duty to ensure that the public has meaningful ways to contribute in the project and to ensure their feedback informs the development of the project.

The next step is to consider an appropriate broadband testing tool. Current public broadband testing tools offer an array of different features. This investigation developed evaluation

criteria to compare different options and to reach a conclusion about the best solution for CIRA. The evaluation criteria has five areas:

1. Tests Conducted – What measurements does the tool employ?
2. Data Storage – How does the tool store the data?
3. Mobile testing – Does the testing solution offer mobile broadband testing?
4. Interface, Mapping and Visualization – How can the tool represent the test and data?
5. Costs – How much does the tool cost?

The following tools were considered for evaluation:

- Switzerland developed by the Electronic Frontier Foundation
- SpeedTest developed by Ookla
- Bredbandskollen by Stiftelsen för Internetinfrastruktur (.SE)
- Measurement Lab testing platform
- Netalyzr developed by International Computer Science Institute
- AquaLab at Northwestern University

Out of these seven possible tools, this investigation explored four broadband testing solutions in depth: SpeedTest, Bredbandskollen, Measurement Labs and the Netalyzr. These tools were considered to have the best potential for a CIRA deployment. The excluded tools were mostly experiments not ready for a large-scale deployment. The only exception was the SamKnows Measurement Platform. This investigation did not consider SamKnows because the tool employs hardware-based testing. Users must install a *whitebox* appliance on their home network unlike the other tools consider that use a web interface. Hardware-based testing has a higher cost of entry since users have to install a *whitebox* and as a result complicates engaging the public. The following section explains the criteria used to evaluation the following tools. Appendix 5.2 includes the detailed comparisons of these four tools. Based on the evaluation,

the best option for CIRA would be to deployment of the Measurement Lab (M-Lab) project. This tool best realizes the vision set forth above, especially in comparison to other options. M-Lab offers an affordable and realizable testing solution for Canada.

The goal of M-Lab is two fold. First, it seeks to expand the testing locations to collect better broadband data from across the globe. Second, it seeks to develop a robust suite of tests and visualizations to help the public research and understand their broadband connection. The project arose in 2008 out of a US-based discussion of the need for more robust broadband measurements. It was developed by Google employees including one of the developers of the Internet Protocols Vint Cerf (Dovrolis et al., 2010). The project was officially announced in January of 2009 as a joint effort of Google, the Open Technology Institute and the PlanetLab Consortium. Today, it is run as an international consortium of corporations, network providers and research institutions. Its members include Google, BitTorrent, PlanetLab, Amazon and Australia's Academic and Research Network. Each agrees to host Measurement Lab servers, individually known as nodes, across the world in service of further broadband research. Appendix 5.1 shows the location of the current nodes. To date, M-Lab has run over 100 million tests since its launch and runs approximately 250,000 tests daily. Most recently, it collaborated with the United States Federal Communications Commission by providing one of two tests for Americans to measure their home Internet connection.

Google and PlanetLab are two integral groups to M-Lab. Google continues to support M-Lab by linking its mapping and data visualization tools to the project and hosting the data collected. PlanetLab, on the other side, is a consortium of academic, industrial and government institutions. The consortium manages the server infrastructure of M-Lab. System administrators from PlanetLab manage each node keeping software up-to-date. Administering distributed nodes fits with PlanetLab's expertise in managing global computer infrastructure.

M-Lab is not a tool or even a service itself, but a platform to conduct Internet research. Since M-Lab is a platform, more so than an actual test project, its servers host a few different and autonomous projects. They differ in their functionality, goals, development team and publication of data. While each depends on the testing infrastructure of M-Lab, most seem to be able to run independent of M-Lab so long as they run the Web100 Linux distribution. In total, six projects have been developed for the M-Lab. Two tools offer advanced upload and download testing (one being NDT), two tools attempt to detect traffic shaping (one being Glasnost) and a third tool focuses on mobile broadband performance. Each also offers some more advanced diagnostics such as determining network congestion. Tools differ not only in their functions, but also their state of development as work for some have ended where others remain in beta testing (Dovrolis et al., 2010)

Through the production of a stable platform, M-Lab provides a base for researchers to develop their own tools. As a platform, Measurement Lab has attracted a number of testing projects that use its infrastructure to measure broadband. For a project to become part of the M-Lab test, it must adhere to its development guidelines. All tools must be open source, release the data to the public domain and adhere to a privacy code of conduct. Its positioning as a platform also applies to data collected as M-Lab releases data into the public domain in two ways: raw logs and a query interface. In sum, M-Lab is a public platform supporting open tools and data.

The M-Lab approach positions CIRA as the platform for broadband testing in Canada. Its infrastructure would ensure that Canadian broadband infrastructure has publicly accessible points of transparency. Even though the project is international, it has no presence in Canada. By deploying M-Lab nodes, CIRA gains international recognition showing its commitment to greater transparency about the Internet for its stakeholders. As well, CIRA would

benefit from the international collaboration around the platform. Its nodes would have the support of the PlanetLab organization, M-Lab and the pool of developers working on the M-Lab platform. Nodes deployed in Canada, especially if part of a larger infrastructure project, would become of the windows of the network, shedding light on the state of the Internet in Canada.

This investigation has identified three components required in a national broadband testing deployment. First, CIRA must build a sufficient infrastructure to support broadband testing. Second, it must develop a website for the public to access and interact with the project. Third, it must promote the project to encourage participation from the public, researchers and policy-makers to expand and improve the tests of the M-Lab. The following section elaborates on the logistics of these three tasks.

The first task involves building M-Lab nodes in Canada to ensure reliable testing nationwide. The best locations based on geography, population and Internet aggregation are: Vancouver, Calgary, Winnipeg, Toronto, Montreal and Halifax. These locations provide the best coverage based on population and geography as shown in Appendix 5.3. Testing nodes must be close to their clients to be reliable. The more hops or networks, a client's test must pass through to connect to the test node, the greater the possibility of an anomalous speed reading (Bauer et al., 2010, pp. 14–15). In addition to being close to a client, nodes should also be located within or near aggregation hubs. All traffic flows toward regional aggregation centres or upstream and then out to the larger international Internet. Locating near these centres would provide the best test of the Canadian network infrastructure. Since there are only two aggregation hubs, CIRA would have to evaluate the future developments of the Canadian backbone when locating nodes (Organisation for Economic Co-operation and Development, 2011, p. 37).

The public would participate in the project through its website. The site would direct visitors to the available testing options. Directions would have to be clear so users know the scope and purpose of their tests. CIRA would have to use some of its adaptation and website development budget to ensure the usability of available tests, particularly NDT and Glasnost. The site might also prompt users to provide some basic demographic information, such as their location, service provider and monthly plan. The site should also provide tutorials for users to understand their tests and to ensure their Internet connection is in working order. In this matter, CIRA has much to learn from the work of .SE who developed a series of video tutorials based on feedback and workshops with end-users. If users express a need for better explanations, then CIRA should consider licensing these videos. Finally, the site should provide users with access to the data through downloading raw logs or aggregated reports, querying data according Big Data Query Language or visual representations. For most users, the site will be a means to understand and explore the data through info-graphics and the Google Public Data Explorer. Appendix 5.4 includes examples of possible visualizations and maps, such as a map of broadband speeds across Canada, IPv6 adoption and instances of traffic shaping.

The M-Lab options for CIRA realizes the vision of a public research project. Measurement Labs is the most open testing solution. Is data go into the public domain and its tools are open source. This openness ensures greater accountability of its test as critics can look at the code. No comparable tool is open source. It offers close to the same amount of tests as the leading Netalyzr. However, unlike Netalyzr that has yet to release the code to its tools, all M-Lab tools are documented and open source. Each has a usable interface, comparable to both Ookla's SpeedTest and Broadband Check. The results can be represented in interactive charts and maps. While the results have international support, the data collected from M-Labs would

have added legitimacy if backed by CIRA. Since M-Lab is more a platform than a specific tool, it promises to have the most longevity of any tool considered. M-Lab creates an open common research platforms that ensures the public has the ability to participate in the study, analysis and extension of a public research project.

Presently, these recommendations have been submitted to CIRA and the board has granted preliminary approval. In the following months, CIRA will move forward according to this plan and deploy a broadband testing infrastructure. However, these recommendations are not an answer, but the beginning of the process. Without a sense of how these technical measures relate to the formation of a public and the constitution of a public memory, then it will be simply a technical exercise in the Internet measurement. A balance exists between the technical considerations of broadband testing and the political task of forming a public. The project, the conclusion argues, must mediate between the two.

A Measurement Lab infrastructure like the one discussed above would compose the kind of public memory necessary for a confrontation with transmissive control. Its NDT and Glasnost tools would both allow for the public to remember the different instances of control and dividuality. These recordings would compose a common memory of the effects of transmissive control and hopefully support public deliberations. Where these recommendations provide a plan for developing a broadband testing infrastructure, it is only important to reflect on the limitations of these methods. This chapter concludes with a sense that technical instruments cannot be the only answer to the challenge of transmissive control. The social sciences must continue to mediate between the technical and the political to ensure that these instruments form the publics necessary to deal with the challenge of transmissive control. These challenges stress the problems of studying algorithmic communication media.

Conclusion: A Plea for the Social Sciences

This chapter shifted between technical matters of Internet measurement to political matters of technology and democracy. It is a strange path not unlike the course of the *Stalker* through the Zone. The stalker of Tarkovsky's film guides two others: a Writer and a Physicist. They paid the stalker to lead them deep into the centre of the Zone. Their differences play off the guide as he struggles to convince them of the Zone and dispel the scepticism carried with them. The end of the film can be interpreted as a success for the stalker as both his companions appear to believe in the Zone. Guides act as mediators between the two; they allow the differing perspectives to agree. The social sciences must act as the same kind of mediator in the study of transmissive control. Public research requires both the sciences and the humanities for the productive balance necessary to publicly study technical systems. This is a balance made taunt by the trajectories of the two approaches.

This chapter had a very clear methodological direction to study transmissive control. The prior section outlines a large-scale public research project. The bulk of the discussion focused on a technical infrastructure – servers and software – in large part because these systems remain the most easy to address. They are a knowable problem with pre-existing solutions; however, they should be seen as a component of a more challenging production of a public reflecting on the challenge of transmissive control. The logs and records generated, analyzed and recorded by this project are just one step. The next is a much greater leap of faith because it requires a public becoming-aware.

A belief in public research arises from a tendency in the work of Dewey toward a scientific democracy. Experimental democratic methods inspire a kind of faith in technical solutions to political problems. Technology disappoints in solving conflict, but also in its appropriation. Wolin argues that the scientific methods exposed by Dewey have been embraced mostly by a

class of political administrators. Those who rely on the science of opinion polls and other instruments to ensure the effective manufacturing of consent. Though Wolin acknowledges the embrace of publics as a predecessor to the civil rights movement, he emphasizes the malleability to technology to totalitarian ends. His warning, in short, stresses that Internet measurement tools always need social mediators, ways to ensure their logging links to the democratic concerns (2004, pp. 518–523).

At the same time, Software Studies tend toward treating software as an object of study, not as a method of study. Certainly, a phenomenological concern needs to address being-encoded or in the words of Barney, the standing reserve of bits. Yet, the expansiveness of a standing reserve, of even the word technology inhibits consideration of software methods to study software. De-compiling, packet sniffing and traceroutes offer software studies, not only as methods, but as projects under the auspices of real study of software and its linkages to humans.

The challenge is that technical tools must not be too instrumentalized. Graeme Wynn addresses the problem of instrumental research in the foreword to the Parr's book *Sensing Changes*. He draws a direct link between embodied perception and the work of McLuhan on media technologies. Explanations of the world, to McLuhan, threaten to detach the observer from the world, where precepts requires participation and engagement (J. Parr, 2010 xii-xiii). Many public research projects already considers human as another computer. One popular project for calculating protein folding switched from digital computing to human computing because "even a small protein can have several hundred amino acids, so computers have to plod through thousands of degrees of freedom to arrive at an optimum energy state. But humans, blessed with a highly evolved talent for spatial manipulation, can often see the solution intuitively" (Hand, 2010, p. 685). Though human intuition offers a markedly different

form of computation, the project considered humans as interchangeable with computers. Terranova (2004) refers to this phenomenon as *free labour* in that humans labour through their intuition, but receive no compensation. Her approach grounded in immaterial labour theory offers a critical basis to question democratic methods. Public research cannot become simply a cheaper computer.

An embrace of software methods must keep in mind the human aspects, the second trajectory of this chapter around publics confronting transmissive control. Parr argues embodied perception sense technological changes. "Our bodies," she writes, "are the instruments through which we become aware of the world beyond our skin, the archives in which we store that knowledge and the laboratories in which we retool our sense and practices to changing circumstance" (2010, p. 1). Most of the investigations into traffic management only began only after human felt as though their connection lagged, but had no evidence to initially prove their claim. Only after their investigation could they prove traffic shaping. In this way, Internet measurement is not an answer to control, but a way of resolving and exploring its effects.

Internet measurement cannot be simply a technical question, it must be a balance between political concerns and social ones. Its participants cannot be simply research subjects, but people experiencing the Internet. Dewey senses the scope of this project when he writes, "the apparatus [of social science] will no longer be taken to be itself knowledge, but will be seen to be intellectual means of making discoveries of phenomena having social import and understanding their meaning" (1927, p. 203). A project constantly finding a balance between the two. Perhaps this approach may be more complicated and messy, but if the proposed project is to avoid the pitfalls outlined by Dewey, it must embrace its messy hybridity, embrace democratic methods and Internment measurement as a cyborg public, one capable of responding and mediating the problems of algorithmic communication media.

This chapter confronts transmissive control through the production of a public memory. Transmissive control, dividuality and the opacity of software obscure the operations of control from the public eye. Users remain fragmented, conflicted and unaware of the operations and implications of transmissive control. The effect is similar to the unseen threats of the Zone – something that requires special means to become aware of. Producing a public memory – a record of transmissive control – requires a project of public research. Publics can become aware of control through collective recording their dividualized experiences into an archive. This archive exposes the working temporal economy of the Internet. It allows dividuals to become aware of their publicity and to reflect on these conditions. Public memory does not answer the problems of transmissive control any more than a public sphere answers the challenges facing a democracy, rather it becomes a first step toward a gradual confrontation with transmissive control.

Public broadband testing tools offer a means to create a public memory of transmissive control. The second half of this chapter discusses the partialities of establishing such a system in Canada. Various options and trajectories had to be considered before recommending that the Canadian Internet Registration Authority (CIRA) deploy a solution based on the Measurement Lab. This dissertation offered a plan for creating and deploying this project as a pragmatic contribution to the challenge of transmissive control. CIRA is currently using this proposal to build this infrastructure. In the near future, Canada might have a means to test and reflect on the operations of transmissive control. It could not come sooner.

Public research also offers an importance place for the social sciences and humanities in the realm of software and computers. It could be a kind of guide exploring the wider social and political consequences of software. This requires a journey beyond its traditional methods and research agendas to confront oblique software. The quantitive opportunities of

digital systems must be measured with qualitative reflection and understanding. Beyond any one direction, the social sciences must seek to use public research to produce new kinds of temporalities for deliberation and debate. This is not necessarily a slow time or a political time, but a temporality that might afford publics to entangle with computers and computer science to come to new collective understandings of the world.

The methods in this chapter offer a way of concluding the concept of transmissive control. It involves a transition from matters of the Internet itself to how their response in a policy environment. In addition to explaining a new concept to understand the Internet, this last chapter demonstrates how transmissive control offers new approaches to the study of the Internet. Both the concept and the software mediators of this chapter hope to spur further research into the nature of transmission. They offer tools that might further unpack the power in the changing conditions of transmission, on the Internet and beyond. Its metaphor of the film *Stalker* gives a sense of the careful and measured steps that must be taken in order understand communication systems full of algorithms and oblique policies.

Chapter Six: Conclusion

Figure 29: "That's Not Fair"

Introduction

An example from a recent advertisement in Canada offers a chance to reflect on the power of transmissive control. One advertisement for Rogers Internet begins with two men siting next to a modern iMac computer. One man appears to be hosting the other. Conversation presumably prompted them to use the Internet. Their motivations for using the Internet, like their computer screen, are hidden to the audience. Action begins with the reaction of the guest to the speed of his host's computer connection. "This is awesome," he exclaims as the scene cuts to an angle showing the computer screen playing an online video. When the guest asks "But I

have the exact same computer and mine is never this fast", the host turns to the camera to explain, "the difference is I have Rogers Internet with their SpeedBoost technology". As he finishes his pitch, his wife appears bringing the two men cups of coffee. She has no speaking role and does not even acknowledge the guest. For approximately five seconds in the twenty-three seconds of the scene, she lovingly caresses her husband and then walks off. All the while, the guest looks at them both, appearing jealous not only of the host's beautiful and attentive wife, but also of the host's superior Internet seen in Figure 29. "That's just not fair" he laments and the host agrees "No, it is not fair". The advertisement aims to convince Canadian consumers to subscribe to Rogers Internet because its SpeedBoost is a technology "you can't get with the other guy's network" (Hollerado - Rogers Commercial, 2011). To the male audience targeted by Rogers Internet, a fast Internet is a status symbol just like an attractive subservient wife.

The advertistement is selling access to tiered Internet capable of modulating transmission depending on usage. Though Rogers Internet claims SpeedBoost results from their cable infrastructure, it is a branded name for a QoS configuration that accelerates short bursts of data resulting in faster speeds for sites like YouTube. Presumably the bandwidth saved through traffic management allows Rogers to momentarily allocate greater rates to these burst communications (see Bauer, Clark, & Lehr, 2011). Roger Internet attempts have created a poly-chronous Internet with a *burst* temporality. The ad depends on convincing its audience that access to this burst temporality is valuable enough to switch to Rogers and situates the wife as another object of desire as part of this status. The guest embodies *the other guy* as he lacks the status of both speed and an attractive wife, but his exclusion is necessary because the valuable burst temporality depends on the *other guy* who moves slowly and lacks status. Rogers produces social stratification through this advertisement and through its SpeedBoost

technology. This stratification exemplifies a poly-chronous Internet, one that regularizes relations and hierarchies within Internet communications. The SpeedBoost bifurcates Internet users into Roger's customers and the other guys.

The product of transmissive control, at first, might be assumed to just control people as the ad suggests. Users pay to access burst speeds or to avoid lag when downloading video games, movies or music. Subscribers wish to buy into a burst temporality for status or convenience. At least Rogers hopes viewers of the ad will buy into their vision of a valuable network as they upgrade their networks to provide SpeedBoost technologies. It highlights an emerging temporality of the Internet. Rogers bursts largely depends on what Internet usages they imagine to be profitable or unprofitable. Rogers Internet does not control people, but the conditions of communication on the Internet.

This ability to set the rates of transmission illustrate that SpeedBoost is more than a new service level or a value-added product – it is a matter of Rogers Internet being able to create a system of control. They are able to orchestrate the moments of resonance and exchange between its customers, its services and its competitors. The product of transmissive control is the production of common moments of cooperation and coordination – temporalities. Transmissions express being-in-communication. Transmission, by assigning temporalities, is an integral factor that sets the tempo of collective becoming and the resonance of the metastability. In the case of Rogers Internet, this control gives them an asymmetrical advantage to create a system of communication that systematically products tiers and rates. The advertisement rightly raises doubts about Rogers Internet as a steward of this transmissive control. Why should Rogers Internet have any dominion over the temporalities of Internet given how much the advertisement seems only interested in perpetuating symbols of status?

This dissertation has provided dream thieves, demons, Ahab and Moby-Dick and the strange land of the Zone as provocations to question the transmissive control employed by Rogers Internet among others. *Inception* provides a context for transmissive control in an asynchronous communication system. The multiple times of the Internet resemble the multiple time of the film. Transmissive control orchestrates these times through the demons of the Internet. Though once in disarray, the conduction of Quality of Service demons seeks to arrange these temporalities into an interrelated economy. Demons seek to turn the asynchronous Internet into a poly-chronous system of temporalities with comparative value. Some – pirates like The Pirate Bay – oppose this shift. They are hunted like how Ahab hunted the White Whale, but by spurring on transmissive control they end up advancing and improving its techniques of control. Instead of the frenzy of escape, the dissertation closes with a metaphor suggesting the need for careful evaluation and a public awareness of transmissive control. The film *Stalker* offers a way to imagine the hidden and instant processes of algorithms as a landscape of the Zone that must be studied and explored. The closing chapter offers a potential response to those displeased with the efforts of Rogers Internet and others. If their activities might be documented and proven, they might eventually be debated and contested as well. Transmissive control, in conclusion, offers the necessary conceptual toolbox to respond to many of the issues facing the Internet.

Contributions

The literature review in the Introduction situated the dissertation into three literatures:

- Communication studies and the concept of control
- Traffic management software and Network Neutrality
- Time, control and technology

The following section explains how the dissertation contributes to each of these sections.

Communication and Control

Communication and control have been challenging concepts to develop if only because the concept of control is much more evasive than normally thought. What does control mean? How does it differ from coercion or force? What does it mean to be under, out of or in control? Typically, answers return to more tangible things like legal contracts or other forms of discipline. Amidst the varieties of control online discussed during the literature review, this dissertation offered the concept of transmissive control to address the influence of software within communication infrastructure. Transmissive control differs from legal contracts or surveillance regimes. Control and transmission concerns a *perpetual metastability* of a system that produces an order through its very conditions of existence. Being able to conceptualize this systematic function of control has been challenging, but also productive in the way it has re-thought the concept of transmission. Control simply implies a means to separate the signal from the noise. As much as this involves control correcting for errors, it does not imagine the actual control during the moment of transmission.

Transmissive control offers a way to understand how temporality can be controlled by algorithms. Transmissive control takes the act of transmission seriously in light of the intensification of advanced Internet routing. How had software and algorithms altered the act of transmission? This has important ramifications for social coordination as it alters the ways of synchronization and the degree of enrolling multiple durations into its temporal economy. Traffic shaping and throttling proved to be the two most evident forms of this control and it certainly has applications in other forms of algorithmic communication. Transmissive control offers a functional concept to explore algorithmic media. This concept questions how soft-

ware remembers the past and enacts goals. In this way, algorithms build on the work of James Beniger (1986) who saw control as a "purposive influence toward a predetermined goal". How to influence depends on a sense of the past to gauge effectiveness and a vision of the future to rationalize its operations. Though the concept of transmissive control has focused on the Internet, it has much greater theoretical opportunities.

The historical section of Chapter Two could not go into enough depth about the particular characteristics of transmission and transmissive control in early telephony or telegraphy. Early computer networks remain a fascinating attempt to create new times through synchronizing humans and computers. These examples point to transmissive control as part of a rich history of media Future research could use the concept of transmissive control to offer a novel history of communication systems or a media archeology of forgotten modes of transmission.

The concept also has rich applications outside the Internet as well. My own future intends to study transmissive control within politics by studying political campaign management software. Real-time control in campaigns is another kind of transmissive control that synchronizes on-demand support, calculated messaging and probabilistic politics. Software acts as a plane of immanence distributed through political campaigns enabling the emergence of nodes; perhaps it allows for a rhizomatic campaign. Software layers control throughout the campaign to convert voter data into profiles that inform tailored messaging. Voter contact involves a synthesis of both algorithms of expression that ensure messages travel as appendages to larger data sets, but also algorithms that create custom content seeking the optimal response from the voter. More in-depth analysis of campaign management software as another kind of algorithm in communication media might offer one direction to the relation of content and expression of transmissive control.

Network Neutrality

Though this dissertation did not attempt to solve the problem of Network Neutrality, it did offer a new vocabulary to address how algorithms produce, resist and confront forms of media power. Studying software challenged conventional research methods, so the dissertation offered new methods to study how digital control re-orients control in communications. Each chapter offers insight into the issue of Network Neutrality by using different objects of study and approaches. Demons, pirates and dosimeters all offer analogies to study the *other* possessing communication media. Demons offered a catalog of the different algorithms circulating on the Internet. They differ in how their perspective and program synthesize a past and a present during transmission. Understanding demons offers critics of traffic shaping a sense of how the potentialities and configurations of demons might undermine the neutrality of networks. These different demons manifested different forms of transmissive control with particular politics. Demons also have limits as seen in the discussion of the escalationism and accelerationism. Such strategies and their capture illustrate the evolution of traffic management software and the different forms of networking online. New controversies, like Network Neutrality, will come from these kinds of struggles. Finally, the last chapter sought to enlist software to expose transmissive control. Public research is a call to action for advocates of a public interest model of the Internet. Software must expose its inner workings. These three chapters provide some methods to understand the software side of Network Neutrality in the hopes to aid the formulation of better policies of Internet regulation.

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.

Time, Control and Technology

This dissertation offers a final contribution in advancing the study of the temporality of the Internet by drawing together the discrete studies into a systematic approach as seen in the concepts of transmissive control, modulating time and temporal economies. Time haunts studies of the Internet. It is an ephemeral characteristic of Internet studies; at once present, yet often overlooked in favour of issues of space. Not only does time remain understudied on the Internet, but so do broader theories of time and power. Most approaches focus on a singular time, such as high-speed or accelerating.

The emphasis on time allows for a new kind of critique of advanced traffic management software. The problem with Internet time, however, is not about its speed. The Deleuzian orientation of this work tends not to have the same concerns with a new time (neuzeit) or fast time since these become part of the multiplicity of times part of the social. The concern is the opposite – time is becoming more predictable. The future horizons narrows under a temporal economy seeking to perpetuate or to realize temporal stratification and relations amidst the modulating time of the Internet.

A more predictable Internet concerns its asynchronicity. It has always been an exciting part of the Internet. It brought together different voices allowing for continual innovation as

seen in the growth of the peer-to-peer network. Amidst a shared belief in the value of an open, high-speed Internet as a medium of open communication and free expression, the Internet collided computer networking into an *internetwork*. It brought together free software programmers, hackers, the venture capitalists of Wired Magazine, the new Right, the techno-utopians of the Whole Earth Catalog, governments, engineers and traditional telecommunication firms forged in an era of common carriage. Asynchronicity has allowed the Internet to be a place of diverse times and ruptures. Beneath terms like *radical innovation* or *killer app* is a sense that the future of the Internet is uncertain and this uncertainty optimistically could be of shared benefit.

A poly-chronous Internet treats the uncertainty of the Internet as a problem. Where once new kinds of packets where since as innovations, QoS increasing treats these packets as the unknown. What is more problematic than a specific traffic management policy for an application is a catch-all filter that slows any unknown or unidentified traffic. The problem with Rogers shaping *World of Warcraft* was not its misclassification of the game, but the fact they had a policy that targeting any unknown peer-to-peer communication. Any unknown or change in Internet routing was treated as a threat that needed to be managed. When William Gibson famously quipped that "the future is already here – it's just not very evenly distributed", he captures the problem of the unknown filter. By managing peer-to-peer traffic before it is understood or has a chance to develop, Rogers forecloses futures to some applications. Transmissive control imposes futures on certain communications. Poly-chronicity offers a concept to question the distribution of futures in a communication system that at-once appears open to innovations and in constant control.

Next Steps

The following section discusses some limitations of the dissertation and some next steps for future research.

Public Research and Software Mediators

Public research is an emerging method that needs to be better situated in a history of participatory research and action research. The relationship between the fields needs greater elaboration than offered by the dissertation. How can the deep commitments of participation and discussion between researchers and subjects translate into the design of software methods and research projects? How can a user running a simple home test be compared to an active research participant? Comparing Internet measurement tools to participatory action research might allow some of the ethical commitments of the approach inform the development of a digital action research project. The risk, as mentioned in Chapter Five, is that Internet measurement tools will enlist humans as cheap computers rather than active participants. This only perpetuates concerns about unaccountable control and a lack of transparency. Future research must go beyond the attempts of public engagement as found in the proposal for public broadband testing tools. How can the public participate around complex areas of technology development? Future research needs to raise these methodological problems in the research design sooner, so that whatever results begins the complex translation of participatory research or action research in the digital era.

Software Studies

Beyond the link between software studies and action research, methods of software studies in general need greater refinement. This dissertation seels to engage in the area of software studies; however, much work remains to hone its approach and to refine its theoretical underpin-

nings. The challenge is doubled because software changes so rapidly that methods become outmoded. Lovink (2008) asks for sustainable concepts applicable to the study of digital networks. Part of the task of sustainability requires software studies to distinguish itself from traditional research methods. Why study software rather than coders or even the effects of code? As well, software studies needs to establish a relationship with what Rogers refers to as digital methods: the use of software to explore digital platforms (cf. Rogers, 2009b). How does studying software differ from studying with software? The solution is approaches which allow software studies to function within triangulations of research in conjunction with interviews or digital methods.

A few unanswered questions emerge out of this dissertation that would aid the formalization of software methods. The first challenge requires a better formulation of the software development cycle. How does a piece of software evolve over time? How does it change from version to version? Beyond the actual product cycle, how can researchers understand the internal developments of software? How and when do developers add or drop features? Deadlines, commercial pressures and sudden innovations all might give a better sense of the information of algorithms. Second, how to understand the political virtualities of software? Most of the time, politics is said to be encoded rather than decoded. Perhaps software might be coded for one reason, but contain a political virtualities that manifest in different directions. Certainly, VPN never anticipated its usage by pirates, but certainly its algorithms readily lend themselves to this cause. How to study the political values beginning with code rather than beginning with how politics informs code? Internet demons arrive loaded on to specific networking appliances that work well with other applications. Advertisements for traffic management software would often highlight how its links with Cisco or Juniper routers. How might the relationality of software be understood so as to create cartographies of network

control? How, in other words, could the potential relations be charted to exposes the flows between software especially the capacities for control between software?

Wireless Networks

Transmissive control offers a way to understand how temporality can be controlled by algorithms. Transmissive control sought to take the act of transmission seriously in light of the intensification of advanced in Internet routing. How had software and algorithms altered the act of transmission? Traffic shaping and throttling proved to be the two most evident forms of this control. It certainly has applications in other communication where algorithms are being introduced. Transmissive control offers a functional concept to question how algorithms function to create temporalities through their management of transmission. While the concept has been applied to the Internet, certainly transmissive control applies to other communication media, such as cellular networks and wireless Internet.

Mobile text messaging offers one potential direction for the study of transmissive control. Research in Motion's (RIM) Blackberry Messaging (BBM) and Apple's iMessage depend on particular systems of transmissive control. Where a simple mobile text message (SMS) offers no feedback, both iMessage and BBM indicate when a user is typing a message and if the user received the message. RIM has long championed BBM in advertising as a way of being connected to its friends. The advertisements clearly sell a kind of mobile real-time economy where subscribers can be in constant contact. To anyone who has complained about their text message not going through or arriving late, the BBM offers notification when a message has been delivered and read. Apple's iMessage does the same. Many analysts regarded Apple's iMessage as a response to BBM – a comparable temporal economy that would afford iPhone users the same benefits as BBM users. It also offered more feedback between users and better

rates of delivery. What other temporal economies circulate amidst smart phones or game consoles if a more rigorous study took place? The case of the Internet offers one foundational case readily applicable to other contexts.

Piracy

Piracy developed in this dissertation largely as an antagonist to transmissive control. Yet, the rise of international Pirate Parties suggest that piracy might be developing into an alternative politics. What are the values of piracy that might translate into political systems? The question is even more important as the German Pirate Party recently won 9% of the total vote in the 2011 election that resulted in 15 seats. It is the first Pirate Party to sit in a state parliament (Dowling, 2011; Ernesto, 2011c). The Berlin Pirate Party now seeks to leverage networked computing into their governance model through a system of transitive proxy voting or what they call *liquid democracy*[39]. Members delegate voting responsibilities to proxies, similar to a representative democracy, but these delegations vary per issue and over time. In effect, proxies create networks with the parties to manifest blocks of support over various positions. Currently, the party is experimenting with deploying the system for internal decisions and debating whether to develop software to facilitate this voting system. Future plans include applying the model to Parliament. Though liquid democracy may appear as a tangent from piracy, its consideration by German pirates involves a translation of Internet values of P2P into political systems. Liquid democracy attempts to create conditions whereby networks might flourish and bloom in the political system akin to how P2P networks have developed online. Liquid democracy embraces the transitive and unfixedness of P2P, but in a political party instead of a digital network. Future research needs to examine the development of these new political projects.

[39] For more details see the Wiki from the project: http://wiki.piratenpartei.de/Liquid_Democracy

Final Words

The Internet is a critical medium to understand transmissive control. The open, decentralized and digital communications network has risen to become a dominant medium across the world. Over one-third of the Earth's seven billion people communicate online (International Telecommunication Union, 2011). Internet traffic will grow by more than thirty precent a year in the future over the next few years (Cisco, 2011). As the Internet engulfs more media and mutates its communications, McLuhan's (1994) vision of a global village intensifies in relevance. As he said, "the world is now like a continually sounding tribal drum, where everybody gets the message all the time" (Millar & O'Leary, 1960). Circuits stretch across the globe as part of the Internet to join regions under a common network tempo. Its messages pulse and set the collective beat for to its users. Packets keep this tempo as they encode and decode messages, but now their rhythms obey a common conductor. The duration of a packet transmission falls under the purposeful direction of networking algorithms. Though packets have always experienced different durations in the network, software now attempts to systemically control their duration.

Algorithms allow for a transmissive control capable of expressing a tiered and stratified temporal economy. It is an orchestration of different temporalities of transmission expressed by transmissive control. Forms of transmission act in concert even though they might operate with different temporalities. The effect is like a jazz ensemble where harmonies emerge even though its players might differ in tempo and tonality. Modulating time refers to the ways Internet Service Provides (ISPs) stratify communications in the present and their ability to do so in the future. Their use of traffic management algorithms create systems of value based on access to different temporalities of communication. Bell Internet exemplifies these changes when it purposely began slowing down peer-to-peer traffic while at the same time promoting

its own digital mall to sell ringtones, movies and music (Kapica, 2008). Without blocking content, Bell prioritized their services, while slowing unprofitable peer-to-peer traffic. Internet Service Providers, such as Bell and Rogers, create temporal economies by tiering Internet speeds that customers pay to access, resulting in the'Network Neutrality controversy (McKelvey, 2010).

Understanding transmissive control "maps not just its strengths, but also its weaknesses. In plotting the nodes and links necessary to capital's flow, it also charts the points where those continuities can be ruptured" (Dyer-Witheford, 1999, p. 92). Network owners have already begun to exert social power utilizing transmissive control. Better network management practices "protect the network from spam, prevent denial-of-service attacks and virus attacks and block access to child pornography sites," stated Ken Engelhart, spokesperson for Rogers Internet in the CRTC hearings on traffic management practices. The Internet must be protected from threats of spam, piracy, viruses, pornography and hackers because of its importance to our daily lives. "Almost every aspect of *our way of life,*" Engelhart adds, "has been transformed by the Internet." His words conflate network management and the public good – protecting the network protects "our way of life". The strategy positions network owners as arbiters of legitimate and illegitimate uses of an open communication network. Thus far, this position has enabled commercial ISPs to monetize Internet communication as part of their profit models and align public opinion to desire this monetization in the name of more efficient networks. A theory of transmissive control offers a way to recognize the politics of traffic management software and to question the future of algorithms in communication media.

Has transmissive control changed since the inception of this dissertation? Bell and Rogers both announced their plans to stop traffic shaping. Does this not imply that the soft control of transmissive control has lost its appeal? Governments in the UK and the Netherlands

launched blockades of The Pirate Bay. Does this not continue a kind of digital enclosure that traffic shaping replaced? OfCom, the FCC and the EU have all gone with a more proprietary, closed source hardware solution to test broadband. Have incumbents grown wary of the potential of public research? Each of these developments certainly complicates the context of transmissive control, but by creating a concept that understands the complexity of algorithms in communication systems. The Internet is one example and a changing example. Amidst the turbulence, the concept of transmissive control endures as an important way to understand the intensification of software within communication systems. Its approach contributes to communication studies by demonstrating the opportunities to integrate software studies into the field and raises questions about the imbrication of software and communication.

Appendices

Appendix 4.1 – BitTorrent MetaData

Source: http://bittorrent.org/beps/bep_0003.html

Metainfo files are encoded dictionaries with the following keys:

announce
The URL of the tracker.

info
This maps to a dictionary, with keys described below.
The name key maps to a UTF-8 encoded string which is the suggested name to save the file (or directory) as. It is purely advisory.

piece length maps to the number of bytes in each piece the file is split into. For the purposes of transfer, files are split into fixed-size pieces which are all the same length except for possibly the last one which may be truncated. piece length is almost always a power of two, most commonly 2 18 = 256 K (BitTorrent prior to version 3.2 uses 2 20 = 1 M as default).

pieces maps to a string whose length is a multiple of 20. It is to be subdivided into strings of length 20, each of which is the SHA1 hash of the piece at the corresponding index.

There is also a key length or a key files, but not both or neither. If length is present then the download represents a single file, otherwise it represents a set of files which go in a directory structure.

In the single file case, length maps to the length of the file in bytes.
For the purposes of the other keys, the multi-file case is treated as only having a single file by concatenating the files in the order they appear in the files list.

The files list is the value files maps to and is a list of dictionaries containing the following keys:

length - The length of the file, in bytes.

path - A list of UTF-8 encoded strings corresponding to subdirectory names, the last of which is the actual file name (a zero length list is an error case).
In the single file case, the name key is the name of a file, in the multiple file case, it's the name of a directory.
All strings in a .torrent file that contains text must be UTF-8 encoded.

Appendix 4.2 – OpenDPI – bittorrent.c

```
/*
 * bittorrent.c
 * Copyright (C) 2009-2010 by ipoque GmbH
 *
 * This file is part of OpenDPI, an open source Deep Packet Inspection
 * library based on the PACE technology by ipoque GmbH
 *
 * OpenDPI is free software: you can redistribute it and/or modify
 * it under the terms of the GNU Lesser General Public License as published
by
 * the Free Software Foundation, either version 3 of the License or
 * (at your option) any later version.
 *
 * OpenDPI is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
 * GNU Lesser General Public License for more details.
 *
 * You should have received a copy of the GNU Lesser General Public License
 * along with OpenDPI. If not, see <http://www.gnu.org/licenses/>.
 *
 */


#include "ipq_protocols.h"
#ifdef IPOQUE_PROTOCOL_BITTORRENT
#define IPOQUE_PROTOCOL_UNSAFE_DETECTION 0
#define IPOQUE_PROTOCOL_SAFE_DETECTION         1

#define IPOQUE_PROTOCOL_PLAIN_DETECTION  0
#define IPOQUE_PROTOCOL_WEBSEED_DETECTION      2
static void ipoque_add_connection_as_bittorrent(struct
ipoque_detection_module_struct

      *ipoque_struct, const u8 save_detection, const u8 encrypted_connection)
{

      struct ipoque_packet_struct *packet = &ipoque_struct->packet;
      struct ipoque_flow_struct *flow = ipoque_struct->flow;
      flow->detected_protocol = IPOQUE_PROTOCOL_BITTORRENT;
      packet->detected_protocol = IPOQUE_PROTOCOL_BITTORRENT;
}

static u8 ipoque_int_search_bittorrent_tcp_zero(struct
ipoque_detection_module_struct

      *ipoque_struct)
{
      struct ipoque_packet_struct *packet = &ipoque_struct->packet;
//  struct ipoque_id_struct *src = ipoque_struct->src;
//  struct ipoque_id_struct *dst = ipoque_struct->dst;

      u16 a = 0;
```

```
      if (packet->payload_packet_len > 20) {
            /* test for match 0x13+"BitTorrent protocol" */
            if (packet->payload[0] == 0x13) {
                  if (memcmp(&packet->payload[1], "BitTorrent protocol", 19)
== 0) {
                        IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT,
                                           ipoque_struct,
IPQ_LOG_TRACE, "BT: plain BitTorrent protocol detected\n");
                        ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_PLAIN_DETECTION);
                        return 1;
                  }
            }
      }

      if (packet->payload_packet_len > 23 && memcmp(packet->payload, "GET
/webseed?info_hash=", 23) == 0) {
            IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT, ipoque_struct,
                                     IPQ_LOG_TRACE, "BT: plain webseed
BitTorrent protocol detected\n");
            ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_WEBSEED_DETECTION);
            return 1;
      }
      /* seen Azureus as server for webseed, possibly other servers existing,
to implement */
      /* is Server: hypertracker Bittorrent? */
/* no asymmetric detection possible for answer of pattern "GET /data?fid=".
*/
      if (packet->payload_packet_len > 60
            && memcmp(packet->payload, "GET /data?fid=", 14) == 0 &&
memcmp(&packet->payload[54], "&size=", 6) == 0) {
            IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT, ipoque_struct,
                                     IPQ_LOG_TRACE, "BT: plain Bitcomet
persistent seed protocol detected\n");
            ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_WEBSEED_DETECTION);
            return 1;
      }


      if (packet->payload_packet_len > 100 && memcmp(packet->payload, "GET ",
4) == 0) {
            const u8 *ptr = &packet->payload[4];
            u16 len = packet->payload_packet_len - 4;
            a = 0;


            /* parse complete get packet here into line structure elements */
            ipq_parse_packet_line_info(ipoque_struct);
            /* answer to this pattern is HTTP....Server: hypertracker */
            if (packet->user_agent_line.ptr != NULL
                  && ((packet->user_agent_line.len > 8 && memcmp(packet-
>user_agent_line.ptr, "Azureus ", 8) == 0)
                        || (packet->user_agent_line.len >= 10 &&
memcmp(packet->user_agent_line.ptr, "BitTorrent", 10) == 0)
```

```
                        || (packet->user_agent_line.len >= 11 &&
memcmp(packet->user_agent_line.ptr, "BTWebClient", 11) == 0))) {
                IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT,
ipoque_struct,
                                                IPQ_LOG_TRACE, "Azureus
/Bittorrent user agent line detected\n");
                ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_WEBSEED_DETECTION);
                return 1;
          }

          if (packet->user_agent_line.ptr != NULL
                && (packet->user_agent_line.len >= 9 && memcmp(packet-
>user_agent_line.ptr, "Shareaza ", 9) == 0)
                && (packet->parsed_lines > 8 && packet->line[8].ptr != 0
                      && packet->line[8].len >= 9 && memcmp(packet-
>line[8].ptr, "X-Queue: ", 9) == 0)) {
                IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT,
ipoque_struct,
                                                IPQ_LOG_TRACE, "Bittorrent
Shareaza detected.\n");
                ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_WEBSEED_DETECTION);
                return 1;
          }

          /* this is a self built client, not possible to catch
asymmetrically */
          if ((packet->parsed_lines == 10 || (packet->parsed_lines == 11 &&
packet->line[11].len == 0))
                && packet->user_agent_line.ptr != NULL
                && packet->user_agent_line.len > 12
                && ipq_mem_cmp(packet->user_agent_line.ptr, "Mozilla/4.0 ",
                                        12) == 0
                && packet->host_line.ptr != NULL
                && packet->host_line.len >= 7
                && packet->line[2].ptr != NULL
                && packet->line[2].len > 14
                && ipq_mem_cmp(packet->line[2].ptr, "Keep-Alive: 300", 15)
== 0
                && packet->line[3].ptr != NULL
                && packet->line[3].len > 21
                && ipq_mem_cmp(packet->line[3].ptr, "Connection: Keep-
alive", 22) == 0
                && packet->line[4].ptr != NULL
                && packet->line[4].len > 10
                && (ipq_mem_cmp(packet->line[4].ptr, "Accpet: */*", 11) == 0
                      || ipq_mem_cmp(packet->line[4].ptr, "Accept: */*", 11)
== 0)

                && packet->line[5].ptr != NULL
                && packet->line[5].len > 12
                && ipq_mem_cmp(packet->line[5].ptr, "Range: bytes=", 13) ==
0
                && packet->line[7].ptr != NULL
                && packet->line[7].len > 15
```

```
                && ipq_mem_cmp(packet->line[7].ptr, "Pragma: no-cache", 16)
== 0
                && packet->line[8].ptr != NULL
                && packet->line[8].len > 22 && ipq_mem_cmp(packet-
>line[8].ptr, "Cache-Control: no-cache", 23) == 0) {

                IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT,
ipoque_struct, IPQ_LOG_TRACE, "Bitcomet LTS detected\n");
                ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_UNSAFE_DETECTION, IPOQUE_PROTOCOL_PLAIN_DETECTION);
                return 1;

          }
          /* answer to this pattern is not possible to implement
asymmetrically */
          while (1) {
                if (len < 50 || ptr[0] == 0x0d) {
                      goto ipq_end_bt_tracker_check;
                }
                if (memcmp(ptr, "info_hash=", 10) == 0) {
                      break;
                }
                len--;
                ptr++;
          }

          IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT, ipoque_struct,
                                    IPQ_LOG_TRACE, " BT stat: tracker info
hash found\n");

          /* len is > 50, so save operation here */
          len -= 10;
          ptr += 10;

          /* parse bt hash */
          for (a = 0; a < 20; a++) {
                if (len < 3) {
                      goto ipq_end_bt_tracker_check;
                }
                if (*ptr == '%') {
                      u8 x1 = 0xFF;
                      u8 x2 = 0xFF;


                      if (ptr[1] >= '0' && ptr[1] <= '9') {
                            x1 = ptr[1] - '0';
                      }
                      if (ptr[1] >= 'a' && ptr[1] <= 'f') {
                            x1 = 10 + ptr[1] - 'a';
                      }
                      if (ptr[1] >= 'A' && ptr[1] <= 'F') {
                            x1 = 10 + ptr[1] - 'A';
                      }

                      if (ptr[2] >= '0' && ptr[2] <= '9') {
                            x2 = ptr[2] - '0';
                      }
```

```
                        if (ptr[2] >= 'a' && ptr[2] <= 'f') {
                              x2 = 10 + ptr[2] - 'a';
                        }
                        if (ptr[2] >= 'A' && ptr[2] <= 'F') {
                              x2 = 10 + ptr[2] - 'A';
                        }

                        if (x1 == 0xFF || x2 == 0xFF) {
                              goto ipq_end_bt_tracker_check;
                        }
                        ptr += 3;
                        len -= 3;
                  } else if (*ptr >= 32 && *ptr < 127) {
                        ptr++;
                        len--;
                  } else {
                        goto ipq_end_bt_tracker_check;
                  }
            }

            IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT, ipoque_struct,
                                     IPQ_LOG_TRACE, " BT stat: tracker info
hash parsed\n");
            ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_PLAIN_DETECTION);
            return 1;
      }

  ipq_end_bt_tracker_check:

      if (packet->payload_packet_len == 80) {
            /* Warez 80 Bytes Packet
             * +----------------+---------------+-----------------
+-----------------+
             * |20 BytesPattern | 32 Bytes Value| 12 BytesPattern | 16 Bytes
Data  |
             * +----------------+---------------+-----------------
+-----------------+
             * 20 BytesPattern : 4c 00 00 00 ff ff ff ff 57 00 00 00 00 00 00
00 20 00 00 00
             * 12 BytesPattern : 28 23 00 00 01 00 00 00 10 00 00 00
             * */
            static const char pattern_20_bytes[20] = { 0x4c, 0x00, 0x00, 0x00,
0xff,
                  0xff, 0xff, 0xff, 0x57, 0x00,
                  0x00, 0x00, 0x00, 0x00, 0x00, 0x20, 0x00, 0x00, 0x00
            };
            static const char pattern_12_bytes[12] = { 0x28, 0x23, 0x00, 0x00,
0x01,
                  0x00, 0x00, 0x00, 0x10, 0x00,
                  0x00, 0x00
            };

/* did not see this pattern anywhere */
            if ((memcmp(&packet->payload[0], pattern_20_bytes, 20) == 0)
                  && (memcmp(&packet->payload[52], pattern_12_bytes, 12) ==
0)) {
```

```
                  IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT,
ipoque_struct,
                                                     IPQ_LOG_TRACE, "BT: Warez - Plain
BitTorrent protocol detected\n");
                  ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_PLAIN_DETECTION);
                  return 1;
            }
      }

      else if (packet->payload_packet_len > 50) {
            if (memcmp(packet->payload, "GET", 3) == 0) {

                  ipq_parse_packet_line_info(ipoque_struct);
/* haven't fount this pattern anywhere */
                  if (packet->host_line.ptr != NULL
                        && packet->host_line.len >= 9 && memcmp(packet-
>host_line.ptr, "ip2p.com:", 9) == 0) {
                        IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT,
                                                      ipoque_struct,
IPQ_LOG_TRACE,
                                                     "BT: Warez - Plain BitTorrent
protocol detected due to Host: ip2p.com: pattern\n");
                        ipoque_add_connection_as_bittorrent(ipoque_struct,

      IPOQUE_PROTOCOL_SAFE_DETECTION, IPOQUE_PROTOCOL_WEBSEED_DETECTION);
                        return 1;
                  }
            }
      }
      return 0;
}


/*Search for BitTorrent commands*/
static void ipoque_int_search_bittorrent_tcp(struct
ipoque_detection_module_struct

*ipoque_struct)
{

      struct ipoque_packet_struct *packet = &ipoque_struct->packet;
      struct ipoque_flow_struct *flow = ipoque_struct->flow;
      if (packet->payload_packet_len == 0) {
            return;
      }

      if (flow->bittorrent_stage == 0 && packet->payload_packet_len != 0) {
            /* exclude stage 0 detection from next run */
            flow->bittorrent_stage = 1;
            if (ipoque_int_search_bittorrent_tcp_zero(ipoque_struct) != 0) {
                  IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT,
ipoque_struct, IPQ_LOG_DEBUG,
                                                "stage 0 has detected something,
returning\n");
                  return;
            }
```

```
            IPQ_LOG_BITTORRENT(IPOQUE_PROTOCOL_BITTORRENT, ipoque_struct,
IPQ_LOG_DEBUG,
                                        "stage 0 has no direct detection, fall
through\n");
      }
      return;
}

void ipoque_search_bittorrent(struct ipoque_detection_module_struct
                                              *ipoque_struct)
{
      struct ipoque_packet_struct *packet = &ipoque_struct->packet;
      if (packet->detected_protocol != IPOQUE_PROTOCOL_BITTORRENT) {
            /* check for tcp retransmission here */

            if ((packet->tcp != NULL)
                  && (packet->tcp_retransmission == 0 || packet-
>num_retried_bytes)) {
                  ipoque_int_search_bittorrent_tcp(ipoque_struct);
            }
      }
}
#endif
```

Appendix 5.1: Locations of M-Lab Nodes Worldwide

Appendix 5.2: Evaluation Criteria

Available Measures by Tool

	Ookla Speedtest	Bredbandskollen	Measurement Lab	Netalyzr
Network Performance				
Download Speed	1	1	1	1
Upload Speed	1	1	1	1
Jitter	1	1	1	1
Latency	1	1	1	1
Packet Loss	1	1	1	1
Buffering / Congestion	0	0	1	1
Network Configuration				
IPv6 Adoption	0	0	1*	1
DNS IPv6	0	0	0	1
DNSSEC	0	0	0	1
DNS Details	0	0	0	1
TraceRoute	0	0	0	1
Interference				
Proxy/Firewall Detection	1	0	1	1
Caching	0	0	0	1
File-type blocking	0	0	1	1
Traffic Shaping	0	0	1	0
Score (out of 15)	6	5	9	14

* In Beta Testing

Mobile Platform Testing

	Ookla Speedtest	Bredbandskollen	Measurement Lab	Netalyzr
Platform				
Apple iOS	1	1	0	0
Google Android	1	1	0	0
RIM Blackberry	1	1	0	0
Windows Mobile				
Score (out of 4)	3	3	0	0

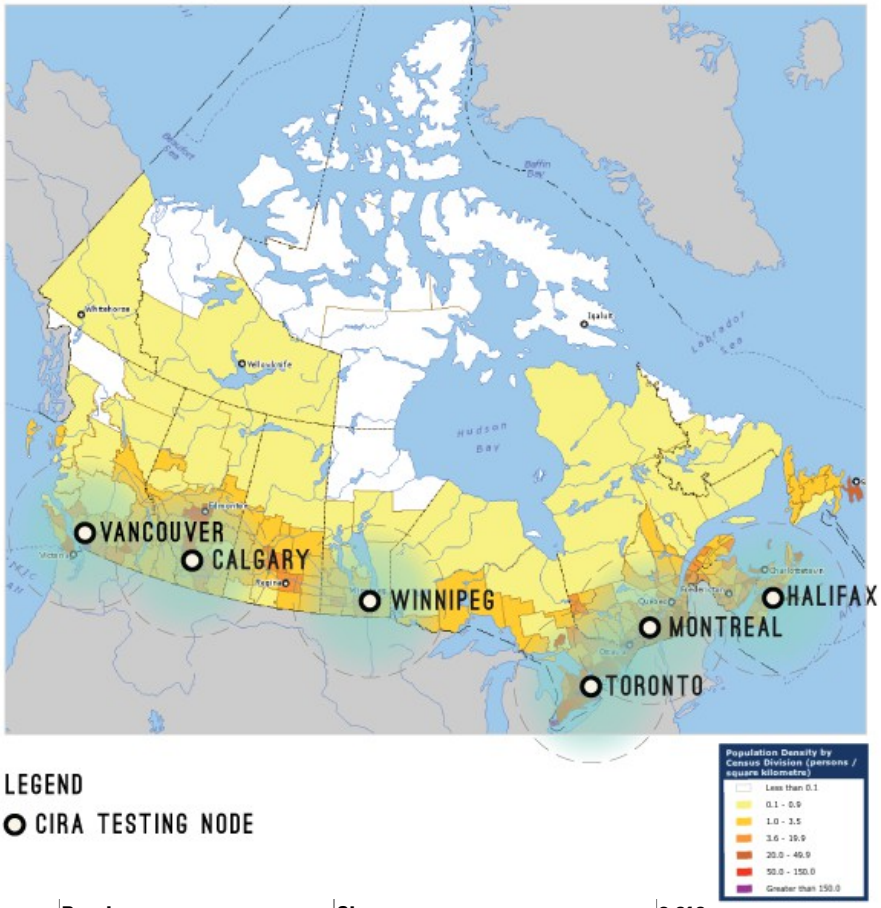
Storage

	Ookla Speedtest	Bredbandskollen	Measurement Lab	Netalyzr
Storage				
Database Format	Database / MySQL	Database / MySQL	Logs / Google Big Query	Amazon EC3
Data Format	Proprietary	Proprietary	Web100 Standard	Unknown
Public Licensing	Creative Commons: Attribution, 0n-Commercial Share Alike	Depends on CIRA, no Canadian data presently available	Public Domain	In process of being made available to the public
Data Collected				
Test Results	1	1	1	1
TCP Dump	0	0	1	0
User Surveys	1	1	0	0
Public Access				
API / Queries	0	0	1	0
Filtered Results	1	1	1	0
Raw Results	0	1	1	0
Data Explorer	1	1	1	0

Visualizations

	Ookla Speedtest	Bredbandskollen	Measurement Lab	Netalyzr
Interface				
Launch Screen	1	1	1	1
Visualized Test	1	1	1	1
Visual Results	1	1	1	0
Mapping				
Mapped Results	0	1	1	0
Scale	N/A	International to Local	International to Local	N/A
Style	N/A	Heat Map	Circle Markers	N/A
Visualization				
Line	1	1	1	0
Bar	1	1	1	0
Motion Chart	1	0	1	0
Score (out of 9)	6	6	7	2

Appendix 5.4: Possible M-Lab Node Locations in Canada



Province	City	2,010
Ontario	Toronto	5,741,419
Quebec	Montréal	3,859,318
British Columbia	Vancouver	2,391,252
Alberta	Calgary	1,242,624
Ontario	Ottawa–Gatineau	1,239,140
Alberta	Edmonton	1,176,307
Quebec	Québec	754,358
Manitoba	Winnipeg	753,555
Ontario	Hamilton	740,238
Ontario	Kitchener–Cambridge–Waterloo	492,390
Ontario	London	492,249
Ontario	St. Catharines–Niagara	404,357
Nova Scotia	Halifax	403,188
Ontario	Oshawa	364,193
British Columbia	Victoria	358,054
Ontario	Windsor	330,856
Saskatchewan	Saskatoon	265,259
Saskatchewan	Regina	215,138
Quebec	Sherbrooke	197,299
Newfoundland	St. John's	192,326

Appendix 5.5: Possible Visualizations for Measurement Lab Test Results

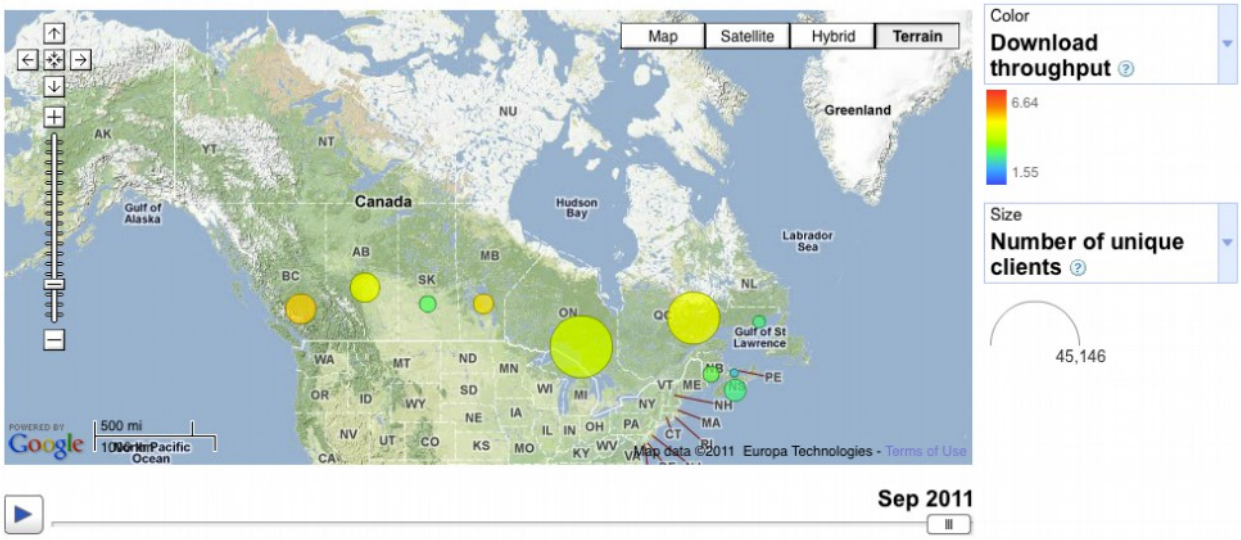


Illustration 1: Download Throughput by Province, the size of the circle increases to represent the number of tests conducted in each provinces and the colour ranges from blue (low download capability) to red (high bandwidth capability) for each circle.

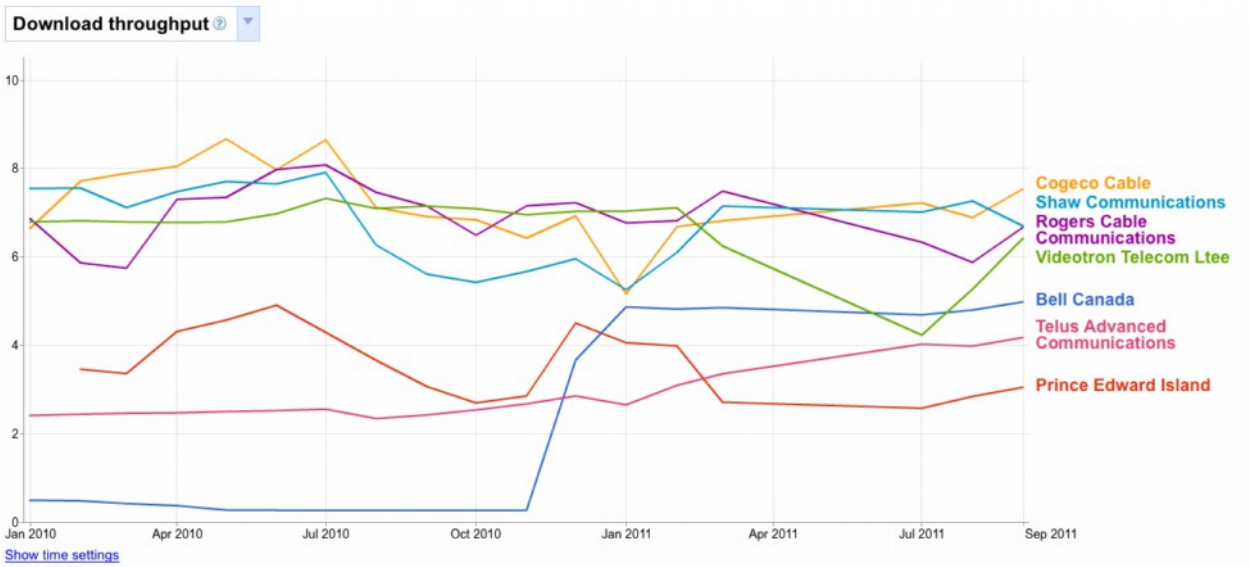


Illustration 2: Download Throughput by ISP

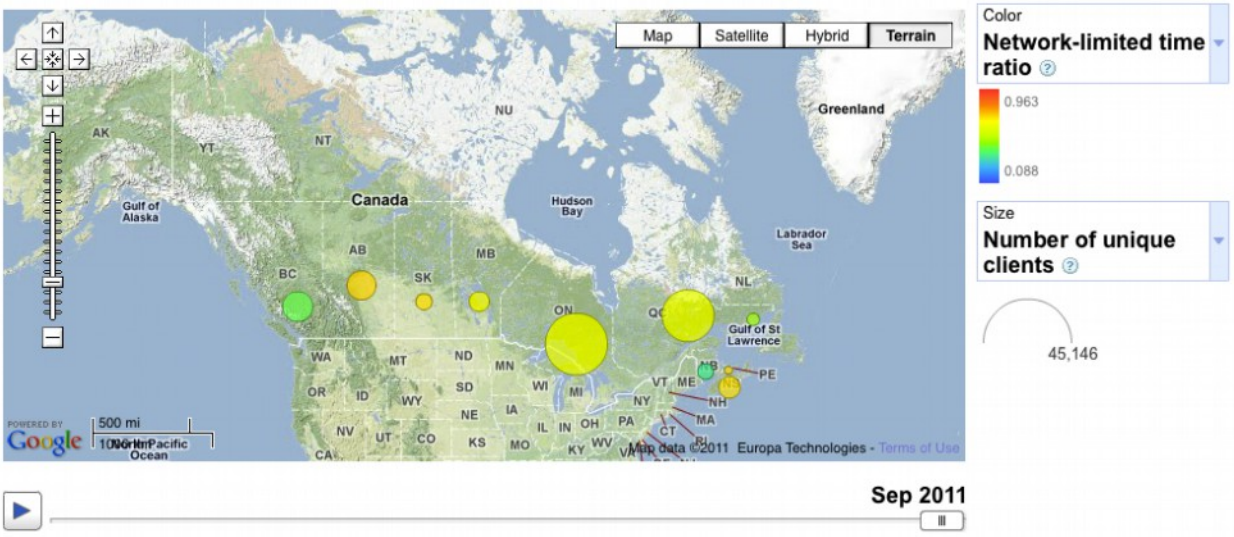


Illustration 3: Congestion by Province, the size of the circle increases to represent the number of tests conducted in each provinces and the colour ranges from blue (low congestion) to red (high congestion) for each circle.

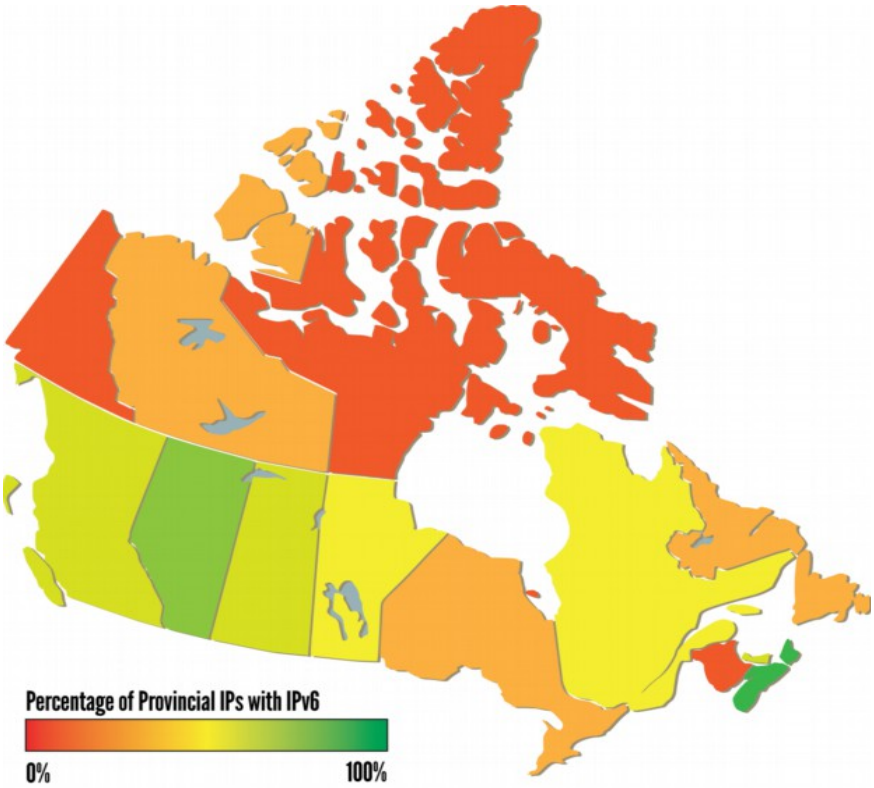


Illustration 4: Possible IPv6 Map

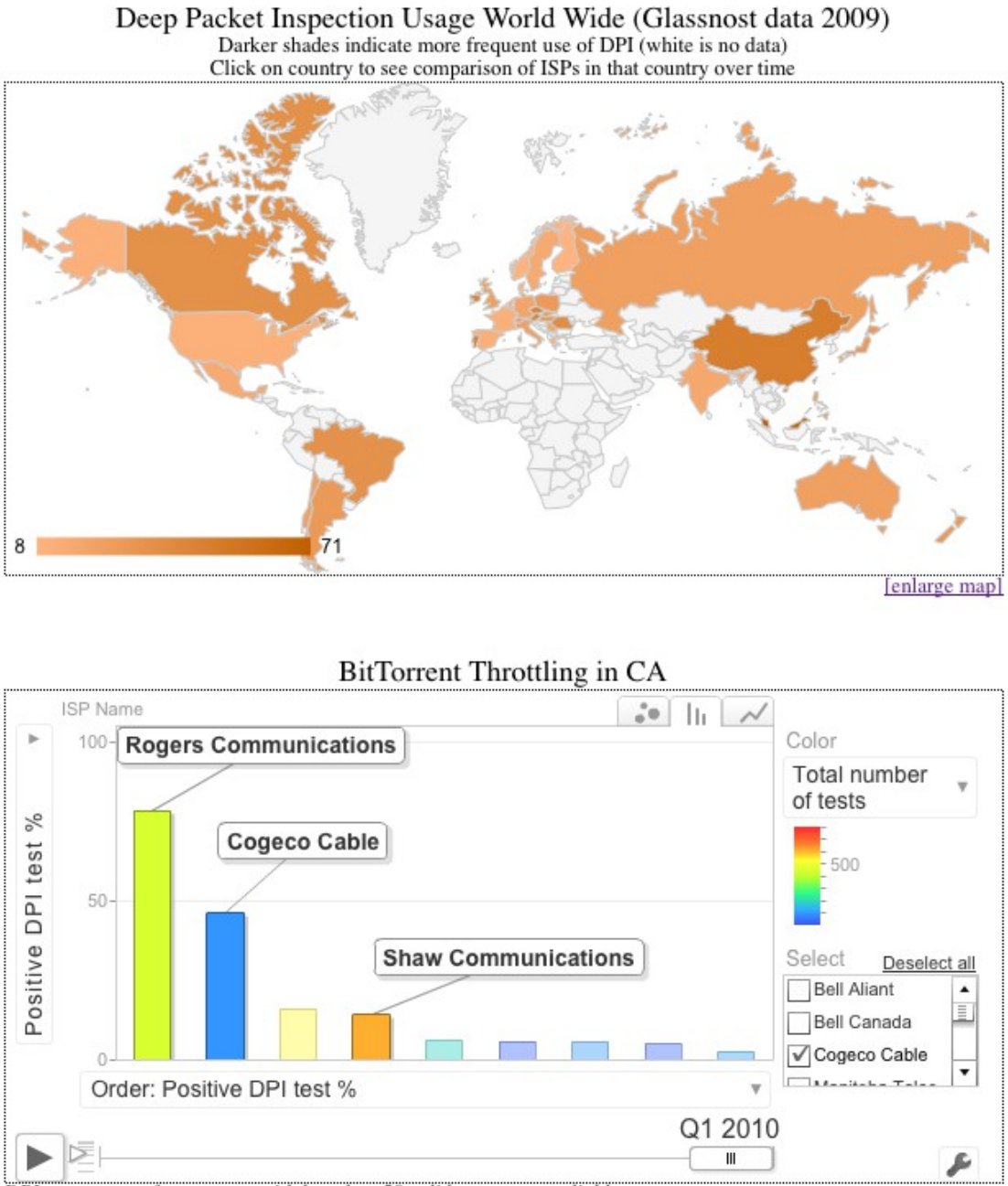


Illustration 5: Traffic Shaping Detection Charting

Bibliography

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

Abbate, J. (2010). Privatizing the Internet: Competing Visions and Chaotic Events, 1987-1995. *IEEE Annals of the History of Computing*, *32*(1), 10–22.

Abbott, A. (2001). *Time Matters: On Theory and Method*. Chicago: University of Chicago Press.

Adam, B. (1990). *Time and Social Theory*. Cambridge: Polity Press.

Adam, B. (2006). Time. *Theory, Culture & Society*, *23*(2-3), 119–126.

Adar, E., & Huberman, B. A. (2000). Free Riding on Gnutella. *First Monday*, *5*(10). Retrieved from http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/792/701

Aitken, P. (2011). Downing Tools in the Media Factory: Online Piracy and the Politics of Refusal. Presented at the Canadian Communications Association, Fredericton.

Albanesius, C. (2009, September 16). Google's M-Lab Now 150K Strong, Adds Support from Greece. Retrieved July 22, 2012, from http://appscout.pcmag.com/google/271596-google-s-m-lab-now-150k-strong-adds-support-from-greece

Alighieri, D. (1851). *Divine Comedy: The Inferno*. New York: Harper & Brothers Publishers. Retrieved from http://books.google.ca/books?id=m5Sl7EpZsC8C

Anderson, N. (2008, March 26). Canadian ISPs furious about Bell Canada's traffic throttling | Ars Technica. Retrieved July 11, 2012, from http://arstechnica.com/uncategorized/2008/03/canadian-isps-furious-about-bell-canadas-traffic-throttling/

Anderson, N. (2011, October 26). House takes Senate's bad Internet censorship bill, tries making it worse. Retrieved October 27, 2011, from http://arstechnica.com/tech-policy/news/2011/10/house-takes-senates-bad-internet-censorship-bill-makes-it-worse.ars

Andersson, J. (2009). For the Good of the Net: The Pirate Bay as a Strategic Sovereign. *Culture Machine*, *10*. Retrieved from http://www.culturemachine.net/index.php/cm/article/view/346/349

Andrejevic, M. (2002). The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure. *Critical Studies in Media Communication*, *12*(2), 230–248.

Angus, I. H. (1998). The Materiality of Expression: Harold Innis' Communication Theory and the Discursive Turn in the Human Sciences. *Canadian Journal of Communication*, *23*(1). Retrieved from http://www.cjc-online.ca/index.php/journal/article/view/1020/926

Angus, I. H. (2001). *Emergent Publics: An Essay on Social Movements and Democracy*. Winnipeg: Arbeiter Ring Pub.

Ansell-Pearson, K. (2002). *Philosophy and the Adventure of the Virtual: Bergson and the Time of Life*. London: Routledge.

Armitage, J., & Graham, P. (2001). Dromoeconomics: Towards a Political Economy of Speed. *Parallax*, *7*(1), 111–123.

Armitage, J., & Roberts, J. (2002a). *Living with Cyberspace: Technology & Society in the 21st Century*. New York: Continuum.

Armitage, J., & Roberts, J. (2002b). Chronotopia. In J. Armitage & J. Roberts (Eds.), (pp. 43–56). New York: Continuum.

Asghari, H., Mueller, M., van Eeten, M., & Wang, X. (2012). *Making Internet Measurements Accessible for Multi-Disciplinary Research An in-depth look at using MLab's Glasnost data for net-neutrality research*. Retrieved from http://dpi.ischool.syr.edu/Papers_files/HA-MM-MvE-IMC.pdf

Ashuri, T. (2012). (Web)sites of memory and the rise of moral mnemonic agents. *New Media & Society*, *14*(3), 441 –456. doi:10.1177/1461444811419636

Aspray, W. (1988). An Annotated Bibliography of Secondary Sources on the History of Software. *Annals of the History of Computing*, *9*(3/4), 291–343.

Atkinson, P. (2009). Henri Bergson. In G. Jones & J. Roffe (Eds.), *Deleuze's Philosophical Lineage* (pp. 237–260). Edinburgh: Edinburgh University Press.

Aughton, S. (2006, October 30). Finnish court frowns on Finreactor BitTorrent | News | PC Pro. Retrieved July 21, 2012, from http://www.pcpro.co.uk/news/96766/finnish-court-frowns-on-finreactor-bittorrent

Austin, G. W. (2005). Importing Kazza - Exporting Grokster. *Santa Clara Computer & High Technology Law Journal*, *22*, 577.

Australia's Academic and Research Network. (2010, June 23). AARNET - News - AARNet and M-Lab bring transparency to Aus broadband networks. Retrieved July 22, 2012, from http://www.aarnet.edu.au/News/2010/06/23/MLab.aspx

Avolio, F. (1999). Firewalls and Internet Security. *The Internet Protocol Journal*, *2*(2). Retrieved from http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html

Bachelard, G. (2000). *The Dialectic of Duration*. (M. M. Jones, Trans.). Manchester: Clinamen.

Bachelard, G. (2008). *The Poetics of Space*. (M. Jolas, Trans.) (Original work published in 1958.). Boston: Beacon Press.

Baran, P. (1962). On Distributed Communications Networks. RAND Corporation.

Baran, P. (1964). On Distributed Communications: 1. Introduction to Distributed Communications Networks. RAND Corporation. Retrieved from http://www.rand.org/pubs/research_memoranda/RM3420.html

Barbrook, R., & Cameron, A. (2001). Californian Ideology. In P. Ludlow (Ed.), (pp. 363–388). Cambridge: MIT Press.

Barney, D. (2000). *Prometheus Wired: The Hope for Democracy in the Age of Network Technology*. Chicago: University of Chicago Press.

Barney, D. (2007). *One Nation Under Google: Citizenship in the Technological Republic*. Toronto: The Hart House Lecture Committee.

Barratt, N., & Shade, L. R. (2007). Net Neutrality: Telecom Policy and the Public Interest, *32*(2), 295–305.

Barry, A., & Slater, D. (2002). Introduction: The Technological Economy. *Economy and Society*, *31*(2), 175–193.

Bauer, S., Clark, D. D., & Lehr, W. H. (2010). *Understanding Broadband Speed Measurements*. Boston: Massachusetts Institute of Technology. Retrieved from http://mitas.csail.mit.edu/papers/Bauer_Clark_Lehr_Broadband_Speed_Measurements.pdf

Bauer, S., Clark, D. D., & Lehr, W. H. (2011). Powerboost. Presented at the Sigcomm Homenets Workshop, Toronto. Retrieved from http://mitas.csail.mit.edu/papers/homenets-bauer-2011.pdf

Beer, D. (2009). Power through the Algorithm? Participatory Web Cultures and the Technological Unconscious. *New Media & Society*, 11(6), 985–1002.

Beer, S. (1974). *Designing Freedom*. London: Wiley.

Beer, S. (1975). *Platform for Change*. London: Wiley.

Bell, A. G. (1876). Improvement in Telegraphy. Salem, Massachusetts.

Bell Canada. (2009a). Comment on Public Notice 2008-19 - Review of the Internet traffic management practices of Internet service providers. Retrieved from http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029804.zip

Bell Canada. (2009b, August 17). Internet Traffic Management. Retrieved from http://www.bell.ca/media/en/all_regions/pdf/Bell_ITM_E_Aug17.09.pdf

Bell Canada. (2011, July 18). *Oral Rebuttal durng Review of usage-based billing for wholesale residential high-speed access service*. Gatineau. Retrieved from http://www.crtc.gc.ca/public/partvii/2011/8661/c12_201102350/1592207.zip

Beller, J. (2006). *The Cinematic Mode of Production: Attention Economy and the Society of the Spectacle*. Lebanon: Dartmouth College Press.

Bellovin, S. M., & Cheswick, W. R. (1994). Network Firewalls. *Communications Magazine, IEEE*, *32*(9), 50–57.

Bendrath, R. (2009). Global Technology Trends and National Regulation: Explaining Variation in the Governance of Deep Packet Inspection.

Bendrath, R., & Mueller, M. (2011). The End of the Net as We Know it? Deep Packet Inspection and Internet Governance. *New Media & Society*, *13*(7), 1142–1160.

Beniger, J. R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Benjamin, W. (1969). *Illuminations: Essays and Reflections*. (H. Zohn, Trans.) (First Schocken paperback ed.). New York: Schocken Books.

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.

Beranek, L. (2000). Roots of the Internet: A Personal History. *Massachusetts Historical Review*, *2*, 55–75.

Berardi, F. (2009). *Precarious Rhapsody: Semocapitalism and the Pathologies of the Post-Alpha Generation*. New York: Autonomedia.

Bergson, H. (1988). *Matter and Memory*. (N. M. Paul & W. S. Palmer, Trans.). New York: Zone Books.

Bettig, R. (1997). The Enclosure of Cyberspace. *Critical Studies in Mass Communications*, *14*(2), 138–158.

BitTorrent Inc. (2009). Comment on Public Notice 2008-19 - Review of the Internet traffic management practices of Internet service providers. Retrieved from http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1249945.PDF

Blom, P. (2010). *A Wicked Company: The Forgotten Radicalism of the European Enlightenment*. New York: Basic Books.

Bolter, J. D., & Grusin, R. (1999). *Remediation: Understanding New Media*. Cambridge: MIT Press.

Brabham, D. C. (2008a). Crowdsourcing as a Model for Problem Solving: An Introduction and Cases. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 75–90. doi:10.1177/1354856507084420

Brabham, D. C. (2008b). Moving the crowd at iStockphoto: The composition of the crowd and motivations for participation in a crowdsourcing application. *First Monday*, *13*(6). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2159/1969

Braman, S. (2003a). From the Modern to the Postmodern: The Future of Global Communications Theory and Research in a Pandemonic Age. In B. Mody (Ed.), *International and Development Communication: A 21st Century Perspective* (pp. 109–123). Thousand Oaks: SAGE Publications.

Braman, S. (Ed.). (2003b). *Communication Researchers and Policy-Making*. Cambridge: MIT Press.

Braman, S., & Roberts, S. (2003). Advantage ISP: Terms of Service as Media Law. *New Media & Society*, *5*(3), 422–448.

Bratich, J. Z. (2006). "Nothing Is Left Alone for Too Long": Reality Programming and Control Society Subjects. *Journal of Communication Inquiry*, *30*(1), 65–83.

Brito, J. (2007). Hack, mash & peer: Crowdsourcing government transparency. *The Columbia Science and Technology Law Review*, *IX*, 119–157.

Brose, H.-G. (2004). An Introduction towards a Culture of Non-Simultaneity? *Time & Society*, *13*(1), 5–26. doi:10.1177/0961463X04040740

Brunton, F., & Nissenbaum, H. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*, *16*(5). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955

Burgess, J., & Green, J. (2009). *YouTube: Online Video and Participatory Culture*. Cambridge: Polity.

Burkart, P. (2012). Cultural Environmentalism and Collective Action: The Case of the Swedish Pirate Party. Presented at the International Communication Association, Phoenix.

Burroughs, W. S. (2000). *Word Virus: the William S. Burroughs Reader*. (J. Grauerholz & I. Silverberg, Eds.). New York: Grove Press.

Bush, R. (1993). FidoNet: Technology, Tools, and History. *Communications of the ACM*, *36*(8), 31–35.

Callon, M. (1998). *The Laws of the Markets*. Oxford: Blackwell Publishers.

Callon, M., Lascoumes, P., & Barthe, Y. (2009). *Acting in an Uncertain World: An Essay on Technical Democracy*. Cambridge: MIT Press.

Callon, M., Méadel, C., & Rabeharisoa, V. (2002). The Economy of Qualities. *Economy and Society*, *31*(2), 194–217.

Campbell-Kelly, M. (1988). Data Communications at the National Physical Laboratory (1965-1975). *IEEE Annals of the History of Computing*, *9*(3/4), 221–247.

Campbell-Kelly, M. (2003). *From Airline Reservations to Sonic the Hedgehog: A History of the Software Industry*. Cambridge: MIT Press.

Campbell-Kelly, M., & Aspray, W. (2004). *Computer: A History of the Information Machine*. Boulder: Westview 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 from http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm

Canadian Radio-television and Telecommunications Commission. (2009a). Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management

practices of Internet service providers. Retrieved from http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm

Canadian Radio-television and Telecommunications Commission. (2009b). Hearings for Review of the Internet traffic management practices of Internet service providers. Retrieved from http://www.crtc.gc.ca/eng/transcripts/2009/tt0706.htm

Cantor, M. G., & Cantor, J. M. (1992). *Prime-time Television: Content and Control*. Thousand Oaks: SAGE Publications.

Cantor, M. G., & Pingree, S. (1983). *The Soap Opera*. Thousand Oaks: SAGE Publications. Retrieved from http://www.loc.gov/catdir/enhancements/fy0660/83011057-d.html

Carey, J. W. (1989). *Communication as Culture: Essays on Media and Society* (Revised Edition, 2009.). New York: Routledge.

Carpo, M. (2011). *The Alphabet and the Algorithm*. Cambridge: MIT Press.

Castells, M. (1996). *The Rise of the Network Society*. Cambridge: Blackwell Publishers.

Cave, D. (2000, October 9). The Mojo solution - Salon.com. Retrieved August 2, 2011, from http://www.salon.com/technology/view/2000/10/09/mojo_nation/index.html

Cerf, V. G. (1991, October). Guidelines for Internet Measurement Activities. Retrieved January 23, 2012, from http://tools.ietf.org/html/rfc1262

Ceruzzi, P. E. (1998). *A History of Modern Computing*. Cambridge: MIT Press.

Ceruzzi, P. E. (2008). The Internet before Commercialization. In W. Aspray & P. E. Ceruzzi (Eds.), (pp. 9–42). Cambridge: MIT Press.

Chandler, J., Davidson, A. I., & Johns, A. (2004). Arts of Transmission: An Introduction. *Critical Inquiry*, *31*(1), 1–6.

Chase, S. (2011, October 27). Privacy watchdog sounds alarm on Conservative e-snooping legislation - The Globe and Mail. Retrieved October 27, 2011, from http://www.theglobeandmail.com/news/politics/ottawa-notebook/privacy-watchdog-sounds-alarm-on-conservative-e-snooping-legislation/article2215907/

Cheng, J. (2009, January 22). Swedish police want personal info of P2P users (Updated) | Ars Technica. Retrieved July 22, 2012, from http://arstechnica.com/tech-policy/2009/01/swedish-police-want-personal-info-of-p2p-users/

Chun, W. (2005). On Software, or the Persistence of Visual Knowledge. *Grey Room*, *Winter*(18), 26–51.

Chun, W. (2006). *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Cambridge: MIT Press.

Chun, W. (2008). Programmability. In M. Fuller (Ed.), *Software Studies: A Lexicon* (pp. 224–229). Cambridge: MIT Press.

Cisco. (2011). VNI Forecast Highlights - Cisco Systems. Retrieved April 5, 2012, from http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html

Cisco Systems. (2002, March 7). Cisco IOS Software Release 11.1CC. *Cisco Systems*. Retrieved July 25, 2012, from http://www.cisco.com/en/US/products/sw/iosswrel/ps1820/products_tech_note09186a00800944ea.shtml

Cisco Systems. (2005). Cisco IOS XR Modular Quality of Service Configuration Guide, Release 3.2. Cisco Systems. Retrieved from http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.2/qos/configuration/guide/qos_c32.html

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

Clark, D. D. (2007). Network Neutrality: Words of Power and 800-Pound Gorillas, 1, 8–20.

Clement, A., Paterson, N., & Phillips, D. J. (2010). IXmaps: Interactively mapping NSA surveillance points in the internet "cloud." Presented at the "A Global Surveillance Society?" Conference, City University, London. Retrieved from http://www.ixmaps.ca/documents/interactively_mapping_paper.pdf

Cohen, B. (2001, July 2). BitTorrent - a new P2P app. *decentralization · Implications of the end-to-end principle*. Retrieved from http://finance.groups.yahoo.com/group/decentralization/message/3160

Cohen, B. (2008). The BitTorrent Protocol Specification. Retrieved July 5, 2011, from http://www.bittorrent.org/beps/bep_0003.html

Connolly, W. E. (2002). *Neuropolitics: Thinking, Culture, Speed*. Minneapolis: University of Minnesota Press.

Conway, F., & Siegelman, J. (2005). *Dark Hero of the Information Age: In search of Norbert Wiener, The Father of Cybernetics*. New York: Basic Books.

Cook, G. (1993). NSFnet Privatization: Policy Making in a Public Interest Vacuum. *Internet Research*, *3*(1), 3–8.

Copeland, D. G., Mason, R. O. ., & Mckenney, J. L. (1995). SABRE: The Development of Information- Based Competence and Execution of Information-Based Competition. *Annals of the History of Computing*, *17*(3), 30–56.

Crary, J. (2001). *Suspensions of Perception: Attention, Spectacle, and Modern Culture*. Cambridge: MIT Press.

Crawford, S. P. (2006). Network Rules. *Cardozo Legal Studies Research Paper*, *159*. Retrieved from http://ssrn.com/paper=885583

Crawford, S. P. (2007). Internet Think. *Journal on Telecommunications and High Technology Law*, *5*(2), 467–468.

Crevier, D. (1993). *AI: The Tumultuous History of the Search for Artificial Intelligence*. New York: Basic Books.

Crocker, S. D. (2009, April 7). How the Internet Got Its Rules. *The New York Times*. Retrieved from http://www.nytimes.com/2009/04/07/opinion/07crocker.html?_r=1&em

Crogan, P. (1999). Theory of State: deleuze, guattari and virilio on the state, technology and speed. *Angelaki*, *4*(2), 137–148.

Dahlberg, L. (2005). The Corporate Colonization of Online Attention and the Marginalization of Critical Communication? *Journal of Communication Inquiry*, *29*(2), 160–180.

Dahlberg, L., & Siapera, E. (Eds.). (2007). *Radical Democracy and the Internet: Interrogating Theory and Practice*. New York: Palgrave Macmillan.

Daly, S. (2007, March). Pirates of the Multiplex. Retrieved from http://www.vanityfair.com/ontheweb/features/2007/03/piratebay200703

Davies, D. (1966). Proposal for a Digital Communication Network. National Physical Laboratory.

Dawkins, R. (1976). *The Selfish Gene*. Oxford: Oxford University Press.

Dean, J. (2008). Communicative Capitalism: Circulation and the Foreclosure of Politics. In M. Boler (Ed.), (pp. 101–122). Cambridge: MIT Press.

Debray, R. (2000). *Transmitting Culture*. (E. Rauth, Trans.). New York: Columbia University Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). Access Denied: The Practice and Policy of Global Internet Filtering. (W. Drake & E. J. Wilson III, Eds.). MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press.

Deibert, R., & Rohozinski, R. (2010). Beyond Denial: Introducing Next-Generation Access Controls. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), (pp. 3–13). Cambridge: MIT Press.

Deleuze, G. (1988). *Foucault*. (S. Hand, Trans.) (Originally work published in 1986.). Minneapolis: University of Minnesota Press.

Deleuze, G. (1989). *Cinema 2:The Time-Image*. (H. Tomilson & R. Galeta, Trans.) (Original work published in 1985.). Minneapolis: University of Minnesota Press.

Deleuze, G. (1990). *Bergsonism*. (H. Tomilson & B. Habberiam, Trans.) (First paperback edition. Original work published in 1966.). New York: Zone Books.

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, *59*(1), 3–7.

Deleuze, G. (1994). *Difference and Repetition*. (P. Patton, Trans.) (Original work published in 1968.). New York: Columbia University Press.

Deleuze, G. (1995a). Control and Becoming. In M. Joughin (Trans.), *Negotiations, 1972-1990* (pp. 169–177). New York: Columbia University Press.

Deleuze, G. (1995b). Mediators. In M. Joughin (Trans.), *Negotiations, 1972-1990* (pp. 121–134). New York: Columbia University Press.

Deleuze, G. (1998a). Having an Idea in Cinema (On the Cinema of Straub-Huillet). In E. Kaufman & K. J. Heller (Eds.), *Deleuze & Guattari: New Mappings in Politics, Philosophy, and Culture* (pp. 14–19). Minneapolis: University of Minnesota Press.

Deleuze, G. (1998b). *Essays Critical and Clinical*. (D. W. Smith & M. A. Greco, Trans.). New York: Verso.

Deleuze, G. (2004). On Gilbert Simondon. In D. Lapoujade (Ed.), *Desert Islands and Other Texts 1953-1974* (pp. 86–89). New York: Semiotext(e).

Deleuze, G. (2007a). What is a Dispositif? In D. Lapoujade (Ed.), *Two Regimes of Madness: Texts and Interviews 1975 - 1995* (Revised ed., pp. 343–352). New York: Semiotext(e).

Deleuze, G. (2007b). *Dialogues II*. (C. Parnet, Ed.). New York: Columbia University Press. Retrieved from http://www.loc.gov/catdir/toc/ecip071/2006031862.html

Deleuze, G., & Guattari, F. (1987). *A Thousand Plateaus: Capitalism and Schizophrenia*. (B. Massumi, Trans.) (Original work published in 1980.). Minneapolis: University of Minnesota Press.

DeMaria, M. J. (2002, January 21). PacketShaper 8500: Traffic management gets smart. *Network Computing*, *13*(2), 22–23.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance*. Cambridge: MIT Press.

Dennis, A. (2002). *Networking in the Internet Age*. New York: John Wiley & Sons, Inc.

Descartes, R. (1996). *Meditations on First Philosophy*. (J. Cottingham, Trans.). New York: Cambridge University Press.

Deseriis, M. (2011). The General, the Watchman, and the Engineer of Control. *Journal of Communication Inquiry*, *35*(4), 387 –394. doi:10.1177/0196859911415677

Deutsch, K. (1966). *The Nerves of Government*. Toronto: Collier-Macmillan Canada.

Dewey, J. (1927). *The Public and its Problems*. Denver: Swallow Press/Ohio University Press.

Dewey, J. (1990). Democratic Ends Need Democratic Methods for Their Realization. In J. A. Boydston & R. W. Sleeper (Eds.), *The Later Works of John Dewey, 1925-1953* (Vol. 14, pp. 367–268). Carbondale: Southern Illinois University Press.

Dinshaw, C., Edelman, L., Ferguson, R. A., Freccero, C., Freeman, E., Halberstam, J., Jagose, A., et al. (2007). THEORIZING QUEER TEMPORALITIES. *GLQ: A Journal of Lesbian and Gay Studies*, *13*(2-3), 177 –195. doi:10.1215/10642684-2006-030

Dischinger, M., Haeberlen, A., Gummadi, K. P., & Saroiu, S. (2007). Characterizing Residential Broadband Networks. *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* (pp. 43–56).

Dischinger, M., Marcon, M., Guha, S., Gummadi, K. P., Mahajan, R., & Saroiu, S. (2010). Glasnost: Enabling end users to detect traffic differentiation. *Proceedings of the 7th USENIX conference on Networked systems design and implementation*.

Dodge, M. (2007). An Atlas of Cyberspaces- Historical Maps. Retrieved June 26, 2012, from http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

Dovrolis, C., Gummadi, K., Kuzmanovic, A., & Meinrath, S. D. (2010). Measurement lab: Overview and an Invitation to the Research Community. *ACM SIGCOMM Computer Communication Review*, *40*(3), 53–56.

Dowling, S. (2011, September 18). Pirate party snatches seats in Berlin state election. *The Guardian*. Retrieved July 22, 2012, from http://www.guardian.co.uk/world/2011/sep/18/pirate-party-germany-berlin-election

Downey, J., & Fenton, N. (2003). New Media, Counter Publicity and the Public Sphere. *New Media & Society*, *5*(2), 185–202.

Duffy, J. (2007a). Cisco's IOS vs. Juniper's JUNOS. Retrieved June 15, 2011, from http://www.networkworld.com/cgi-bin/mailto/x.cgi?pagetosend=/news/2008/041708-cisco-juniper-operating-systems.html&pagename=/news/2008/041708-cisco-juniper-operating-systems.html&pageurl=http://www.networkworld.com/news/2008/041708-cisco-juniper-operating-systems.html&site=printpage&nsdr=n

Duffy, J. (2007b). Cisco IOS vs. Juniper JUNOS: The Technical Differences. Retrieved June 15, 2011, from http://www.networkworld.com/cgi-bin/mailto/x.cgi?pagetosend=/news/2008/041708-cisco-juniper-operating-systems-side.html&pagename=/news/2008/041708-cisco-juniper-operating-systems-side.html&pageurl=http://www.networkworld.com/news/2008/041708-cisco-juniper-operating-systems-side.html&site=printpage&nsdr=n

Dusi, M., Crotti, M., Gringoli, F., & Salgarelli, L. (2008). Detection of encrypted tunnels across network boundaries. *Communications, 2008. ICC'08. IEEE International Conference on* (pp. 1738–1744).

Dyer-Witheford, N. (1999). *Cyber-Marx: Cycles and Circuits of Struggle in High-Technology Capitalism*. Urbana: University of Illinois Press.

Dyer-Witheford, N. (2002). E-Capital and the Many-Headed Hydra. In G. Elmer (Ed.), *Critical Perspectives on the Internet* (pp. 129–164). Lanham: Rowman & Littlefield.

Edwards, P. N. (1997). *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge: MIT Press.

Edwards, P. N. (2003). Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems. In T. J. Misa, P. Brey, & A. Feenberg (Eds.), (pp. 185–226). Cambridge: MIT Press.

Elias, N. (1992). *Time: An Essay*. Oxford: Blackwell Publishers.

Ellis, D. (2011, September 21). Game throttled? Complain about Rogers, but blame the CRTC | Life on the Broadband Internet. Retrieved September 23, 2011, from http://www.davidellis.ca/2011/09/21/game-throttled-complain-about-rogers-but-blame-the-crtc/

Elmer, G. (2002). The Case of Web Browser Cookies: Enabling/Disabling Convenience and Relevance on the Web. In G. Elmer (Ed.), (pp. 49–62). Lanham: Rowman & Littlefield.

Elmer, G. (2004). *Profiling Machines: Mapping the Personal Information Economy*. Cambridge: MIT Press.

Elsenaar, A., & Scha, R. (2002). Electric body manipulation as performance art: A historical perspective. *Leonardo music journal*, *12*, 17–28.

emceeology. (1999, December 27). Name Some Banging tunes !! *alt.rap*. Retrieved from https://groups.google.com/forum/?hl=en&fromgroups#!topic/alt.rap/KliJffM3N1k

Eriksson, M. (2006, October 14). Speech for Piratbyrån @ Bzoom festival in Brno, Czech rep. Retrieved August 3, 2011, from http://fadetogrey.wordpress.com/2006/10/14/brno/

Ernesto. (2010a, June 23). Pirate Bay's Founding Group "Piratbyrån" Disbands | TorrentFreak. Retrieved August 3, 2011, from http://torrentfreak.com/pirate-bays-founding-group-piratbyran-disbands-100623/

Ernesto. (2010b, November 26). The Pirate Bay Appeal Verdict: Guilty Again | TorrentFreak. Retrieved July 22, 2012, from http://torrentfreak.com/the-pirate-bay-appeal-verdict-101126/

Ernesto. (2011a, April 19). Pirate Party Canada Launch VPN to Fight Censorship | TorrentFreak. Retrieved July 22, 2012, from http://torrentfreak.com/pirate-party-canada-launch-vpn-to-fight-censorship-110419/

Ernesto. (2011b, May 16). The Pirate Bay Ships New Servers to Mountain Complex | TorrentFreak. Retrieved July 21, 2012, from http://torrentfreak.com/the-pirate-bay-ships-new-servers-to-mountain-complex-110516/

Ernesto. (2011c, September 18). Pirate Party Enters Berlin Parliament After Historic Election Win | TorrentFreak. Retrieved September 23, 2011, from http://torrentfreak.com/pirate-party-enters-berlin-parliament-after-historical-election-win-110918/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29

Ezrahi, Y. (1999). Dewey's Critique of Democratic Visual Culture and Its Political Implications. In D. Kleinberg-Levin (Ed.), *Sites of Vision: The Discursive Construction of Sight in the History of Philosophy* (pp. 315–336). Cambridge: MIT Press.

Falk, H. (1984). The Source v. CompuServe. *Online Information Review*, *8*(3), 214–224.

Finnie, G. (2009). ISP Traffic Management Technologies: The State of the Art. Heavy Reading. Retrieved from http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm

Fiveash, K. (2012, January 5). Official: File-sharing is a religion... in Sweden • The Register. Retrieved January 11, 2012, from http://www.theregister.co.uk/2012/01/05/file_sharing_sweden_kopimism_religion/

Fleischer, R. (2006, December 12). Between artworks and networks: Navigating through the crisis of copyright << Copyriiot. Retrieved from http://copyriot.wordpress.com/2006/12/12/between-artworks-and-networks/

Fleischer, R. (2010, January 13). COPYRIOT | Pirate politics: from accelerationism to escalationism? Retrieved August 3, 2011, from http://copyriot.se/2010/01/13/pirate-politics-from-accelerationism-to-escalationism/

Fleischer, R., & Palle, T. (2007, May 15). The Grey Commons. Retrieved from http://www.piratbyran.org/index.php?view=articles&id=107&cat=3

Fleisher, R. (2008, February 4). "Indexing the Grey Zone": A Talk at Transmediale08. Retrieved from http://copyriot.se/2008/02/04/indexing-the-grey-zone-a-talk-at-transmediale08/

Foucault, M. (1978). *Discipline & Punish: The Birth of the Prison*. (A. Sheridan, Trans.) (2nd Edition, 1995. Original work published in 1975.). New York: Vintage.

Foucault, M. (2007). *Security, Territory, Population: Lectures at the College de France, 1977-78*. (G. Burchell, Trans.). New York: Palgrave Macmillan.

Fraser, N. (1992). Rethinking the Public Sphere: A Contribution to the Critique of Actual Democracy. In C. J. Calhoun (Ed.), (pp. 109–142). Cambridge: MIT Press.

Freeman, E. (2010). *Time Binds: Queer Temporalities, Queer Histories*. Durham: Duke University Press.

Frieden, R. (2002). Revenge of the Bellheads: How the Netheads Lost Control of the Internet. *Telecommunications Policy*, *26*(7-8), 425–444.

Fuller, M. (2008a). Introduction. In M. Fuller (Ed.), *Software Studies: A Lexicon* (pp. 1–14). Cambridge: MIT Press.

Fuller, M. (Ed.). (2008b). *Software Studies: A Lexicon*. Cambridge: MIT Press.

Fulmer, C. E. (2006). When Discrimination Is Good: Encouraging Broadband Internet Investment Without Content Neutrality. Retrieved from http://www.law.duke.edu/journals/dltr/articles/PDF/2006DLTR0006.pdf

Galison, P. L. (1994). The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision. *Critical Inquiry*, *21*(1), 228–266.

Galison, P. L. (2003). *Einstein's Clocks, Poincaré's Maps: Empires of Time*. New York: Norton.

Galloway, A. R. (2004). *Protocol: How Control Exists After Decentralization*. Cambridge: MIT Press.

Galloway, A. R. (2006). *Gaming: Essays on Algorithmic Culture*. Minneapolis: University of Minnesota Press.

Galloway, A. R., & Thacker, E. (2004). Protocol, Control, and Networks. *Grey Room*, *17*(Fall), 6–29.

Galloway, A. R., & Thacker, E. (2007). *The Exploit: A Theory of Networks*. Minneapolis: University of Minnesota Press.

Garde-Hansen, J., Hoskins, A., & Reading, A. (Eds.). (2009). *Save As... Digital Memories*. New York: Palgrave Macmillan.

Geertz, C. (1973). *The Interpretation of Cultures: Selected Essays*. New York: Basic Books.

Geist, M. (2008a). Network Neutrality in Canada. *For Sale to the Highest Bidder: Telecom Policy in Canada* (pp. 73–82). Ottawa: Canadian Centre for Policy Alternatives.

Geist, M. (2008b, November 24). CRTC ruling not the last word on Net neutrality - thestar.com. Retrieved July 11, 2012, from http://www.thestar.com/sciencetech/article/542156

Geist, M. (2009, October 21). Michael Geist - CRTC Sets Net Neutrality Framework But Leaves Guarantees More Complaints. Retrieved July 12, 2012, from http://www.michaelgeist.ca/content/view/4478/125/

Geist, M. (2011a, June 29). Michael Geist - Canada's Net Neutrality Enforcement Failure. Retrieved July 11, 2011, from http://www.michaelgeist.ca/content/view/5918/159/

Geist, M. (2011b, June 29). Michael Geist - CRTC Faces Charges of Bias in Online Video Consultation. Retrieved July 10, 2012, from http://www.michaelgeist.ca/content/view/5900/135/

Geist, M. (2011c, November 14). Geist: Lawful access legislation would reshape Canada's Internet - thestar.com. Retrieved October 27, 2011, from http://www.thestar.com/news/sciencetech/technology/lawbytes/article/889359--geist-lawful-access-legislation-would-reshape-canada-s-internet

Gerovitch, S. (2004). *From Newspeak To Cyberspeak: A History Of Soviet Cybernetics*. Cambridge: MIT Press.

Gerovitch, S. (2008). InterNyet: why the Soviet Union did not build a nationwide computer network. *History and Technology*, *24*(4), 335–350. doi:10.1080/07341510802044736

Giacomello, G., & Picci, L. (2003). My scale or your meter? Evaluating methods of measuring the Internet. *Information Economics and Policy*, *15*(3), 363–383. doi:10.1016/S0167-6245(03)00003-9

Gillespie, T. (2006a). Designed to "effectively frustrate": copyright, technology and the agency of users. *New Media & Society*, *8*(4), 651–669.

Gillespie, T. (2006b). Engineering a Principle: "End-to-End" in the Design of the Internet. *Social Studies of Science*, *36*(3), 427–457.

Gillespie, T. (2007). *Wired Shut: Copyright and the Shape of Digital Culture*. Cambridge: MIT Press.

Gillespie, T. (2010). The Politics of "Platforms." *New Media & Society*, *12*(3), 347–364.

Goffey, A. (2008). Algorithm. In M. Fuller (Ed.), *Software Studies: A Lexicon* (pp. 15–20). Cambridge: MIT Press.

Goldhaber, M. H. (1997). The Attention Economy and the Net. *First Monday*, *2*(4). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/519/440

Gore Jr., A. (1989). Congressional Record: Presentation on the National High-Performance Computer Technology Act. *ACM SIGGRAPH Computer Graphics*, *23*(4), 276.

Gore Jr., A. (1991). Infrastructure for the Global Village. *Scientific American*, *265*(3), 150–153.

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

Greenberg, A. (2011, December 26). Meet Telecomix, The Hackers Bent On Exposing Those Who Censor And Surveil The Internet - Forbes. Retrieved July 22, 2012, from http://www.forbes.com/sites/andygreenberg/2011/12/26/meet-telecomix-the-hackers-bent-on-exposing-those-who-censor-and-surveil-the-internet/

Grier, D. A., & Campbell, M. (2000). A Social History of Bitnet and Listserv, 1985-1991. *IEEE Annals of the History of Computing*, *22*(2), 32–41.

Guillory, J. (2004). The Memo and Modernity. *Critical Inquiry*, *31*(1), 108–132.

Guins, R. (2009). *Edited Clean Version: Technology and the Culture of Control*. Minneapolis: University of Minnesota Press.

Halavais, A. (2009). *Search Engine Society*. Cambridge: Polity.

Hamzeh, K., Pall, G. S., Verthein, W., Taarud, J., Little, W. A., & Zorn, G. (1999). RFC 2637 - Point-to-Point Tunneling Protocol (PPTP) (RFC2637). Retrieved July 22, 2012, from http://www.faqs.org/rfcs/rfc2637.html

Hand, E. (2010). Citizen Science: People Power. *Nature*, (466), 685–687.

Hart, J. A. (2011). The Net Neutrality Debate in the United States. *Journal of Information Technology & Politics*, *8*, 418–443. doi:10.1080/19331681.2011.577650

Hassan, R. (2007). Network Time. In R. Hassan & R. E. Purser (Eds.), *24/7: Time and Temporality in the Network Society* (pp. 37–61). Stanford: Stanford University Press.

Hassan, R. (2009). *Empires of Speed: Time and the Acceleration of Politics and Society*. Leiden: Brill.

Hassan, R., & Purser, R. E. (Eds.). (2007). *24/7: Time and Temporality in the Network Society*. Stanford: Stanford University Press.

Hayles, N. K. (1999). *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: University of Chicago Press.

Heavy Reading. (2011). DPI Appliance Vendors Face an Off-the-Shelf Challenge. Retrieved October 27, 2011, from http://www.heavyreading.com/insider/details.asp?sku_id=2741&skuitem_itemid=1348&promo_code=&aff_code=&next_url=%2Finsider%2Flist%2Easp%3Fpage%5Ftype%3Drecent%5Freports

Heidegger, M. (1962). *Being and Time*. (J. Macquarrie & E. Robinson, Trans.) (Original work published in 1927.). New York: Harper.

Heidegger, M. (1977). *The Question Concerning Technology, and Other Essays*. New York: Harper & Row.

Heimann, P. M. (1970). Molecular forces, statistical representation and Maxwell's demon. *Studies In History and Philosophy of Science Part A*, 1(3), 189–211. doi:10.1016/0039-3681(70)90009-9

Hellsten, L., Leydesdorff, L., & Wouters, P. (2006). Multiple Presents: How search engines rewrite the past. *New Media & Society*, 8(6), 901–924. doi:10.1177/1461444806069648

Hobson, D. (2003). *Soap Opera*. Cambridge: Polity. Retrieved from http://www.loc.gov/catdir/toc/fy0602/2002072835.html

Hollerado - Rogers Commercial. (2011). Retrieved from http://www.youtube.com/watch?v=ws7wcJaX75k&feature=youtube_gdata_player

Hookway, B. (1999). *Pandemonium: The Rise of Predatory Locales in the Postwar World*. New York: Princeton Architectural Press.

Hörning, K. H., Ahrens, D., & Gerhard, A. (1999). Do Technologies have Time?: New Practices of Time and the Transformation of Communication Technologies. *Time & Society*, 8(2-3), 293–308. doi:10.1177/0961463X99008002005

Howe, J. (2006). Wired 14.06: The Rise of Crowdsourcing. Wired Magazine. Retrieved from http://www.wired.com/wired/archive/14.06/crowds_pr.html

Huston, G. (1999). *ISP Survival Guide: Strategies for Running a Competitive ISP*. New York: Wiley. Retrieved from http://www.loc.gov/catdir/description/wiley033/98038660.html

Huurdeman, A. A. (2003). *The Worldwide History of Telecommunications*. New York: Wiley.

Ibarrola, E., Liberal, F., & Ferro. (2010). An Analysis of Quality of Service Architectures: Principles, Requirements, and Future Trends. In P. Bhattarakosol (Ed.), *Intelligent Quality of Service Technologies and Network Management: Models for Enhancing Communication* (pp. 15–35). Hershey: IGI Global.

Ingham, K., & Forrest, S. (2006). Network Firewalls. In V. R. Vemuri (Ed.), (pp. 9–35). Boca Raton: Auerbach Publications. Retrieved from http://www.loc.gov/catdir/enhancements/fy0647/2005047840-d.html

Innis, H. A. (1950). *Empire and Communications*. Oxford: Clarendon Press.

Innis, H. A. (1951). *The Bias of Communication* (2nd ed.). Toronto: University of Toronto Press.

International Telecommunication Union. (2011). *The World in 2011: ICT Facts and Figures*. Geneva: International Telecommunication Union. Retrieved from http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

Introna, L., & Nissenbaum, H. (2000). The Public Good Vision of the Internet and the Politics of Search Engines. In R. Rogers (Ed.), (pp. 25–48). Maastricht: Jan van Eyck Akadamie.

ipoque. (2012). Datasheet: PACE Protocol & Application Classification Engine. Retrieved July 22, 2012, from http://www.ipoque.com/sites/default/files/mediafiles/documents/data-sheet-pace.pdf

Irwin, A. (1995). *Citizen Science: A Study of People, Expertise and Sustainable Development*. New York: Routledge.

Isenberg, D. S. (1998). The Dawn of the "Stupid network." *netWorker*, *2*(1), 24–31.

Jacobs, J. E. (1983). SAGE Overview. *Annals of the History of Computing*, *5*(4), 4.

Johns, A. (2010). *Piracy: The Intellectual Property Wars from Gutenberg to Gates*. Chicago: University of Chicago Press.

Johnston, J. (1999). Machinic Vision. *Critical Inquiry*, *26*(1), 25–45.

Jones, B. (2007, January 24). The Pirate Bay in the Hot Seat | TorrentFreak. Retrieved August 3, 2011, from http://torrentfreak.com/the-pirate-bay-in-the-hot-seat/

Jones, R. (2000). Digital Rule: Punishment, Control and Technology. *Punishment & Society*, *2*(1), 5–22.

Jowett, G., Jarvie, I. C., & Fuller, K. H. (1996). *Children and the Movies: Media Influence and the Payne Fund Controversy*. Cambridge: Cambridge University Press.

Kahn, R., & Cerf, V. (2000, September 29). <nettime> Al Gore and the Internet. Retrieved from http://amsterdam.nettime.org/Lists-Archives/nettime-l-0009/msg00311.html

Kan, G. (2001). Gnutella. In A. Oram (Ed.), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (pp. 94–122). Sebastopol: O'Reilly.

Kane, C. L., & Peters, J. D. (2010). Speaking Into the iPhone: An Interview With John Durham Peters, or, Ghostly Cessation for the Digital Age. *Journal of Communication Inquiry*, *34*(2), 119–133. doi:10.1177/0196859910365908

Kapica, J. (2008). Bell opens a large can of worms. Retrieved from http://v1.theglobeandmail.com/servlet/story/RTGAM.20080521.WBcyberia20080521192217/WBStory/WBcyberia

Karaganis, J. (2007). The Ecology of Control: Filters, Digital Rights Management, and Trusted Computing. In J. Karaganis (Ed.), (pp. 256–281). New York: Social Science Research Council.

Katz, L. (2012, July 5). *Speech to the Canadian Telecom Summit*. Presented at the Canadian Telecom Summit, Toronto. Retrieved from http://www.crtc.gc.ca/eng/com200/2012/s120605.htm

Kelty, C. (2008). *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press.

Kirschenbaum, M. G. (2000). Hypertext. In T. Swiss (Ed.), (pp. 120–137). New York: New York University Press.

Kiss, J. (2009, April 17). The Pirate Bay trial: guilty verdict | Technology | guardian.co.uk. Retrieved July 22, 2012, from http://www.guardian.co.uk/technology/2009/apr/17/the-pirate-bay-trial-guilty-verdict

Kita, C. I. (2003). J.C.R. Licklider's vision for the IPTO. *IEEE Annals of the History of Computing*, *25*(3), 62–77. doi:10.1109/MAHC.2003.1226656

Kittler, F. (1995). There is No Software. Retrieved from http://www.ctheory.net/articles.aspx?id=74#bio

Kleinrock, L. (1978a). Principles and Lessons in Packet Communications. *Proceedings of the IEEE*, *66*(11), 1320–1329.

Kleinrock, L. (1978b). On Flow Control in Computer Networks. *Conference Record, Proceedings of the International Conference on Communications* (Vol. II, pp. 27.2.1–27.2.5). Toronto, Ontario.

Kleinrock, L. (2010). An Early History of the ARPANET. *IEEE Communications Magazine*, *48*(8), 26–36.

Kline, S., Dyer-Witheford, N., & Peuter, G. de. (2003). *Digital Play: The Interaction of Technology, Culture, and Marketing*. Montreal: McGill-Queen's University Press.

Kravets, D. (2008, January 8). FCC Opens File-Sharing Probe (Charade) Into Comcast Traffic-Management Practices | Threat Level | Wired.com. Retrieved July 11, 2012, from http://www.wired.com/threatlevel/2008/01/fcc-opens-file/

Kreibich, C., Weaver, N., Nechaev, B., & Paxson, V. (2010). Netalyzr: Illuminating The Edge Network. Presented at the Internet Measurement Conference 2010, Melbourne, Australia. Retrieved from http://www.icir.org/christian/publications/2010-imc-netalyzr.pdf

Kurs, S. (2007). Yo ho ho -buccanerds give studios a broadside. *Sunday Times*, p. 6. London (UK), United Kingdom, London (UK).

Land, C. (2007). Flying the Black Flag: Revolt, Revolution and The Social Organization of Piracy in the `Golden Age'. *Management & Organizational History*, *2*(2), 169–192.

Langlois, G. (2011). Meaning, Semiotechnologies and Participatory Media. *Culture Machine*, *12*.

Langlois, G., Elmer, G., McKelvey, F., & Devereaux, Z. (2009). Networked Publics: The Double Articulation of Code and Politics on Facebook. *Canadian Journal of Communication*, *34*(3), 415–433.

Langlois, G., McKelvey, F., Elmer, G., & Werbin, K. (2009). Mapping Commercial Web 2.0 Worlds: Towards a New Critical Ontogenesis. *Fibreculture*, *14*.

Lanham, R. A. (2006). *The Economics of Attention: Style and Substance in the Age of Information*. Chicago: University of Chicago Press.

Lasar, M. (2011, September 19). Canada to Rogers Cable: we want fix for game throttling by next week | Ars Technica. Retrieved July 22, 2012, from http://arstechnica.com/tech-policy/2011/09/canada-to-rogers-cable-fix-game-throttling-by-friday/

Lash, S. (2002). *Critique of Information*. Thousand Oaks: SAGE Publications.

Lash, S. (2007). Power after Hegemony: Cultural Studies in Mutation? *Theory, Culture & Society*, *24*(3), 55–78.

Latham, R. (2005). Networks, Information, and the Rise of the Global Internet. In R. Latham & S. Sassen (Eds.), (pp. 146–177). Princeton: Princeton University Press.

Latham, R. (2010). Border formations: security and subjectivity at the border. *Citizenship Studies*, *14*(2), 185–201. doi:10.1080/13621021003594858

Latham, R. (2012). Circulation and Identity Across the Liberal Citadel. Presented at the Colloquium: Foucault/Deleuze: A Neo-Liberal Diagram, Ryerson University, Toronto, Canada.

Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge: Harvard University Press.

Latour, B. (2004). *Politics of Nature: How to Bring the Sciences into Democracy*. Cambridge: Harvard University Press.

Latour, B. (2005). From Realpolitik to Dingpolitik or How to Make Things Public. In B. Latour & P. Weibel (Eds.), (pp. 14–41). Cambridge: MIT Press.

Lawson, S. (2008, September 21). Blue Coat to Acquire Packeteer for $268 Million | PCWorld. Retrieved July 5, 2011, from http://www.pcworld.com/printable/article/id,144902/printable.html

Lazzarato, M. (1996). Immaterial Labour. Retrieved from http://www.generation-online.org/c/fcimmateriallabour3.htm

Lazzarato, M. (2003). Struggle, Event, Media. Republic Art. Retrieved from http://www.republicart.net/disc/representations/lazzarato01_en.htm

Lazzarato, M. (2007). Machines to Crystallize Time: Bergson. *Theory, Culture & Society*, *24*(6), 93–122.

Lee, J. A. N. (1992). Claims to the Term "Time-Sharing." *IEEE Annals of the History of Computing*, *14*(1), 16–17.

Lee, T. B. (2008). The Durable Internet: Preserving Network Neutrality without Regulation. *Cato Institute Policy Analysis*, *626*.

Lefebvre, H. (2004). *Rhythmanalysis: Space, Time and Everyday Life*. (S. Elden & G. Moore, Trans.) (First Continuum Edition. Original work published in 1992.). New York: Continuum.

Legout, A., Urvoy-Keller, G., & Michiardi, P. (2005). Understanding bittorrent: An experimental perspective. *INRIA Sophia Antipolis/INRIA Rhne-Alpes-PLANETE INRIA France, EURECOM-Institut Eurecom, Tech. Rep*.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., et al. (1997). The Past and Future History of the Internet. *Communications of the ACM*, *40*(2), 102–108.

Leong, S., Mitew, T., Celletti, M., & Pearson, E. (2009). The Question Concerning (Internet) Time. *New Media & Society*, *11*(8), 1267–1285.

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

Lewis, J. (2001). *Constructing Public Opinion: How Political Elites Do What They Like and Why We Seem to Go Along with It*. New York: Columbia University Press.

Leyshon, A. (2003). Scary monsters? Software Formats, Peer-to-Peer Networks, and the Spectre of the Gift. *Environment and Planning D: Society and Space*, *21*(5), 533–558.

Li, M. (2009). The Pirate Party and The Pirate Bay: How The Pirate Bay Influences Sweden and International Copyright Relations. *Pace International Law Review*, *21*(1), 281.

Licklider, J. C. R. (1960). Man-Computer Symbiosis. *Human Factors in Electronics, IRE Transactions on*, *HFE-1*(1), 4–11.

Licklider, J. C. R. (1963, April 23). Memorandum For Members and Affiliates of the Intergalactic Computer Network. Advanced Projects Research Agency. Retrieved from http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network

Licklider, J. C. R., & Taylor, R. W. (1968). The Computer as a Communication Device, *76*, 21–31.

Lindgren, S., & Linde, J. (2012). The Subpolitics of Online Piracy: A Swedish case study. *Convergence: The International Journal of Research into New Media Technologies*, *18*(2), 143–164. doi:10.1177/1354856511433681

Lippmann, W. (1922). *Public Opinion* (First Free Press Paperbacks edition, 1997.). New York: Free Press Paperbacks.

Loft, A. (1995). "Time is money." *Culture and Organization*, *1*(1), 127–145.

Lovink, G. (2008). *Zero Comments: Blogging and Critical Internet Culture*. New York: Routledge. Retrieved from http://www.loc.gov/catdir/toc/ecip0711/2007005611.html

Lukasik, S. J. (2011). Why the ARPANET was Built. *IEEE Annals of the History of Computing*, *33*(3), 4–21.

Lyman, P. (2004). Information Superhighways, Virtual Communities, and Digital Libraries: Information Society as Political Rhetoric. In M. Sturken, D. Thomas, & S. Ball-Rokeach (Eds.), (pp. 201–218). Philadelphia: Temple University Press.

Lyons, M. (1985). Primary Internet Gateways - 1985 June 18. Retrieved June 26, 2012, from http://www.livinginternet.com/i/ii_arpanet_gateways.htm

Mackenzie, A. (2002). *Transductions: Bodies and Machines at Speed*. New York: Continuum.

Mackenzie, A. (2006). Java: The Practical Virtuality of Internet Programming. *New Media & Society*, *8*(3), 441–465.

Mackenzie, A. (2007). Protocols and the Irreducible Traces of Embodiment: The Viterbi Algorithm and the Mosaic of Machine Time. In R. Hassan & R. E. Purser (Eds.), *24/7: Time and Temporality in the Network Society* (pp. 89–105). Stanford: Stanford University Press.

Mackenzie, A. (2010). *Wirelessness: Radical Empiricism in Network Cultures*. Cambridge: MIT Press.

Manovich, L. (2002). *The Language of New Media*. Cambridge: MIT Press.

Mansell, R. (1993). *The New Telecommunications: A Political Economy of Network Evolution.* Thousand Oaks: Sage Publications.

Maras, S. (2008). On Transmission: A Metamethodological Analysis (after Régis Debray). *Fibreculture*, (12). Retrieved from http://twelve.fibreculturejournal.org/fcj-080-on-transmission-a-metamethodological-analysis-after-regis-debray/

Marres, N. (2004). Tracing the Trajectories of Issues, and their Democratic Deficits, on the Web. *Information Technology and People*, *17*(2), 124–149.

Marres, N. (2005). Issues Spark a Public into Being: A Key But Often Forgotten Point of the Lippmann-Dewey Debate. In B. Latour & P. Weibel (Eds.), (pp. 208–217). Cambridge: MIT Press.

Marres, N. (2010). Front-staging Nonhumans: Publicity as a Constraint on the Political Activity of Things. In B. Braun & S. J. Whatmore (Eds.), *Political Matter: Technoscience, Democracy, and Public Life* (pp. 177–210). Minneapolis: University of Minnesota Press.

Marsden, C. (2010). *Net Neutrality: Towards a Co-Regulatory Solution*. London: Bloomsbury Publishing. Retrieved from http://ssrn.com/abstract=1533428

Marvin, C. (1988). *When Old Technologies were New: Thinking about Electric Communication in the Late Nineteenth Century*. New York: Oxford University Press.

Masnick, M. (2011, October 26). PROTECT IP Renamed E-PARASITES Act; Would Create The Great Firewall Of America | Techdirt. Retrieved October 27, 2011, from http://www.techdirt.com/articles/20111026/12130616523/protect-ip-renamed-e-parasites-act-would-create-great-firewall-america.shtml

Massumi, B. (2002a). *Parables for the Virtual: Movement, Affect, Sensation*. Durham: Duke University Press.

Massumi, B. (2002b). A Shock to Thought: Expression after Deleuze and Guattari. Routledge.

Mattelart, A. (1996). *The Invention of Communication*. Minneapolis: University of Minnesota Press.

Mattelart, A. (2000). *Networking the World, 1794-2000*. Minneapolis: University of Minnesota Press.

Mattelart, A. (2003). *The Information Society: An Introduction*. London: Sage.

Maxwell, J. (1872). *Theory of Heat*. New York: D. Appleton and Co.

May, J., & Thrift, N. (Eds.). (2001). *TimeSpace: Geographies of Temporality*. London: Routledge.

Mayer-Schonberger, V. (2011). *Delete: the Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press. Retrieved from http://public.eblib.com/EBLPublic/PublicView.do?ptiID=686418

McConnell, M. (2011, February 28). Mike McConnell on how to win the cyber-war we're losing. Retrieved October 27, 2011, from http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

McCoy, J. (2001, January 11). Mojo Nation Responds - O'Reilly Media. Retrieved September 23, 2011, from http://openp2p.com/pub/a/p2p/2001/01/11/mojo.html

McCullagh, D. (2000, July 29). Get Your Music Mojo Working. Retrieved August 2, 2011, from http://www.wired.com/science/discoveries/news/2000/07/37892

McIver Jr., W. (2010). Internet. In M. Raboy & J. Shtern (Eds.), (pp. 145–174). Vancouver: UBC Press.

McKelvey, F. (2010). Ends and Ways: The Algorithmic Politics of Network Neutrality. *Global Media Journal - Canadian Edition*, *3*(1), 51–73.

McKelvey, F. (2011). A Programmable Platform? Drupal, Modularity, and the Future of the Web. *Fibreculture*, (18). Retrieved from http://eighteen.fibreculturejournal.org/2011/10/09/fcj-128-programmable-platform-drupal-modularity-and-the-future-of-the-web/

McLuhan, M. (1994). *Understanding Media: The Extensions of Man* (First MIT Press edition. First published in 1964.). Cambridge: MIT Press.

McStay, A. (2010). Profiling Phorm: an autopoietic approach to the audience-as-commodity. *Surveillance & Society*, *8*(3), 310–322.

McTaggart, C. (2006). Was the Internet Ever Neutral? Presented at the Research Conference on Communication, Information and Internet Policy, Arlington, USA.

McTaggart, C. (2008). Net Neutrality and Canada's Telecommunications Act. Presented at the National Conference on New Developments in Communications Law and Policy, Ottawa, Canada.

Medina, E. (2011). *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. Cambridge: MIT Press.

Menzies, H. (2005). *No Time: Stress and the Crisis of Modern Life*. Vancouver: Douglas & McIntyre.

Middleton, C. (2007). *Understanding the Benefits of Broadband: Insights for a Broadband Enabled Ontario*. Ontario: Ministry of Government Services. Retrieved from http://www.broadbandresearch.ca/ourresearch/middleton_BB_benefits.pdf

Miegel, F., & Olsson, T. (2008). From Pirates to Politician: The Story of the Swedish File Sharers who became a Political Party. In N. Carpentier, P. Pruulmann-Vengerfeldt, K. Nordenstreng, M. Hartmann, P. Vihalemm, B. Cammaerts, H. Nieminen, et al. (Eds.), *Democracy, Journalism and Technology: New Developments in an Enlarged Europe* (pp. 203–217). Tartu: Tartu Publisher Press.

Millar, A., & O'Leary, J. (1960, May 18). The Global Village. *Explorations*. CBC. Retrieved from http://www.cbc.ca/archives/categories/arts-entertainment/media/marshall-mcluhan-the-man-and-his-message/world-is-a-global-village.html

Mindell, D. A. (2002). *Between Human and Machine: Feedback, Control, and Computing before Cybernetics*. Baltimore: Johns Hopkins University Press.

Molyneux, R., & Williams, R. (1999). Measuring the Internet. *Annual Review of Information Science and Technology* (Vol. 34). Medford: Information Today, Inc.

Moschovitis, C. J. P. (1999). *History of the Internet: A Chronology, 1843 to the Present*. Santa Barbara, Calif.: ABC-CLIO.

Mosco, V. (1996). *The Political Economy of Communication: Rethinking and Renewal*. Thousand Oaks: SAGE Publications.

Moya, J. (2008, July 9). Swedish Prosecutor Won't Investigate Top Cop's MPAA Ties. Retrieved July 22, 2012, from http://www.zeropaid.com/news/9622/swedish_prosecutor_wont_investigate_top_cops_mpaa_ties/

Mueller, M. (2002). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: MIT Press.

Mueller, M. (2010). *Networks and States: the Global Politics of Internet Governance*. Cambridge: MIT Press.

Mueller, M., & Asghari, H. (2011). Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States. *Telecommunications Policy Research Conference*. Arlington.

Mulgan, G. J. (1991). *Communication and Control: Networks and the New Economies of Communication*. New York: Guilford Press.

Mumford, L. (1934). *Technics and Civilization*. New York: Harcourt, Brace.

Murphy, B. M. (2002). A Critical History of the Internet. In G. Elmer (Ed.), (pp. 27–45). Lanham: Rowman & Littlefield.

Murray, M., & claffy, kc. (2001). Measuring the Immeasurable: Global Internet Measurement Infrastructure. *In PAM – A workshop on Passive and Active Measurements* (pp. 159–167).

Needham, T. (1746). Extract of a Letter from Mr. Turbervill Needham to Martin Folkes, Esq; Pr. R. S. concerning Some New Electrical Experiments Lately Made at Paris. *Philosophical Transactions*, *44*(478-484), 247 –263. doi:10.1098/rstl.1746.0050

Noble, D. F. (1984). *Forces of Production: A Social History of Industrial Automation*. New York: Knopf.

Norberg, A. L., & O'Neill, J. E. (1996). *Transforming Computer Technology: Information Processing for the Pentagon, 1962-1986*. Baltimore: Johns Hopkins University Press. Retrieved from http://0-hdl.handle.net.biblio.eui.eu/2027/heb.01152

Norton, Q. (2006, August 16). Secrets of The Pirate Bay. Retrieved August 3, 2011, from http://www.wired.com/science/discoveries/news/2006/08/71543

Nowak, P. (2008a, April 22). Cogeco ranks poorly in internet interference report - Technology & Science - CBC News. Retrieved July 11, 2012, from http://www.cbc.ca/news/technology/story/2008/04/22/tech-vuze.html

Nowak, P. (2008b, May 15). CRTC opens net neutrality debate to public - Technology & Science - CBC News. Retrieved July 10, 2012, from http://www.cbc.ca/news/technology/story/2008/05/15/tech-internet.html

O'Neill, J. E. (1995). The Role of ARPA in the Development of the ARPANET, 1961-1972. *IEEE Annals of the History of Computing*, *17*(4), 76–81.

Oram, A. (2001). Peer-to-peer: Harnessing the Benefits of a Disruptive Technology. O'Reilly.

Organisation for Economic Co-operation and Development. (2011). *Internet Traffic Exchange: Market Developments and Policy Challenges*. Paris: Organisation for Economic Co-operation and Development.

Orlowski, A. (2011, October 26). BT gets 14 days to block Newzbin2 • The Register. Retrieved October 27, 2011, from http://www.theregister.co.uk/2011/10/26/bt_newsbin2_block_get_on_with_it/

Orman, H. (2003). The Morris Worm: a Fifteen-year Perspective. *Security & Privacy, IEEE*, *1*(5), 35–43.

Packeteer, Inc. (2001). Packeteer's PacketShaper/ISP. Retrieved from http://archive.icann.org/en/tlds/org/applications/unity/appendices/pdfs/packeteer/PSISP_colorB1101.pdf

Packeteer, Inc. (2002). Packetshaper Packetseeker Getting Started Guide. Retrieved from https://bto.bluecoat.com/packetguide/5.3.0/documents/PacketShaper_Getting_Started_v53.pdf

Parikka, J. (2007). Contagion and Repetition: On the Viral Logic of Network Culture. *Ephemera: Theory and Politics in Organisation*, *7*(2).

Parikka, J. (2010). *Insect Media: An Archaeology of Animals and Technology*. Minneapolis: University of Minnesota Press.

Parr, A. (Ed.). (2005). Becoming. *The Deleuze Dictionary*. Edinburgh: Edinburgh University Press.

Parr, J. (2010). *Sensing Changes: Technologies, Environments, and the Everyday, 1953-2003.* Vancouver: UBC Press.

Parsons, C. (2008). Deep Packet Inspection in Perspective: Tracing its Lineage and Surveillance Potentials. New Transparency Project. Retrieved from https://qspace.library.queensu.ca/bitstream/1974/1939/1/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf

Parsons, C. (2009, June 29). Draft: What's Driving Deep Packet Inspection in Canada? | Technology, Thoughts, and Trinkets. Retrieved October 27, 2011, from http://www.christopher-parsons.com/blog/thoughts/draft-whats-driving-deep-packet-inspection-in-canada/

Parsons, C. (2011, March 6). Literature Review of Deep Packet Inspection. New Transparency Project's Cyber - Surveillance Workshop. Retrieved from http://www.christopher-parsons.com/blog/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf

Paterson, N. (2009). Bandwidth is Political: Reachability in the Public Internet. York University.

Patowary, K. (2010, June 18). Security flaw makes PPTP VPN useless for hiding IP on BitTorrent - Instant Fundas. Retrieved July 22, 2012, from http://www.instantfundas.com/2010/06/security-flaw-makes-pptp-vpn-useless.html

Paul, I. (2010, March 12). FCC Offers Free Broadband Speed Test. *PCWorld*. Retrieved July 22, 2012, from http://www.pcworld.com/article/191398/fcc_offers_free_broadband_speed_test.html

Paxson, V. (1999). End-to-end internet packet dynamics. *IEEE/ACM Transactions on Networking (TON)*, *7*(3), 277–292.

Paxson, V. (2004). Strategies for sound Internet measurement. *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement* (pp. 263–271).

Peha, J. M., & Lehr, W. H. (2007). Introduction: The State of the Debate on Network Neutrality. *International Journal of Communication*, *1*(1).

Peters, J. D. (1988). Information: Notes Toward a Critical History. *Journal of Communication Inquiry*, *12*(2), 9–23.

Peters, J. D. (1996). The Uncanniness of Communication in Interwar Social Thought. *Journal of Communication*, *46*(3), 108–123.

Poster, M. (2001). CyberDemocracy: The Internet and the Public Sphere. In D. Trend (Ed.), (pp. 259–271). Malden: Blackwell Publishers.

Powell, A., & Cooper, A. (2011). Net Neutrality Discourses: Comparing Advocacy and Regulatory Arguments in the United States and the United Kingdom. *The Information Society*, *27*(5), 311–325. doi:10.1080/01972243.2011.607034

Prasad, R., Dovrolis, C., Murray, M., & Claffy, K. (2003). Bandwidth Estimation: Metrics, Measurement Techniques, and Tools. *Network, IEEE*, *17*(6), 27– 35.

Procera Networks. (n.d.). PRE - PacketLogic Real-Time Enforcement. Retrieved July 22, 2012, from http://www.proceranetworks.com/plr-packetlogic-real-time-enforcement/

Purdy, D. (2010, June 7). *Business Models 3.0*. Presented at the Canadian Telecom Summit, Toronto.

Quail, C., & Larabie, C. (2010). Net Neutrality: Media Discourses and Public Perception. *Global Media Journal - Canadian Edition*, *3*(1), 31–50.

Quarterman, J. S., & Hoskins, J. C. (1986). Notable Computer Networks. *Communications of the ACM*, *29*(10), 932–971.

Rakow, L. F. (1992). *Gender on the Line: Women, the Telephone and Community Life*. Chicago: University of Illinois Press.

Randell, B. (1979). An Annotated Bibliography of the Origins of Digital Computers. *Annals of the History of Computing*, *1*(2), 101–207.

Raymond, E. S. (Ed.). (1996). Demon. *The New Hacker's Dictionary*. Cambridge: MIT Press.

Redmond, K. C., & Smith, T. M. (2000). *From Whirlwind to MITRE : the R&D story of the SAGE air defense computer*. Cambridge: MIT Press.

Rheingold, H. (2000). *The Virtual Community: Homesteading on the Electronic Frontier*. Cambridge: MIT Press.

Ripeanu, M., Mowbray, M., Andrade, N., & Lima, A. (2006). Gifting Technologies: A BitTorrent Case Study. *First Monday*, *11*(11). Retrieved from http://firstmonday.org/issues/issue11_11/ripeanu/index.html

Roberts, L. G. (1978). The Evolution of Packet Switching. *Proceedings of the IEEE*, *66*(11), 1307–1313.

Robinson, D. (2008). Variable. In M. Fuller (Ed.), *Software Studies: A Lexicon* (pp. 260–266). Cambridge: MIT Press.

Roderick, I. (2007). (Out of) Control Demons: Software Agents, Complexity Theory and the Revolution in Military Affairs. *Theory & Event*, 10(2).

Rogers Communications. (2009a). Comment on Public Notice 2008-19 - Review of the Internet traffic management practices of Internet service providers. Retrieved 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 from http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1005723.zip

Rogers Communications. (2012). Rogers Network Management Policy - Rogers. Retrieved July 22, 2012, from http://www.rogers.com/web/content/network_management

Rogers, R. (2004). *Information Politics on the Web*. (Anonymous, Ed.). Cambridge: MIT Press.

Rogers, R. (2009a). The Internet Treats Censorship as a Malfunction and Routes Around It?: A New Media Approach to the Study of State Internet Censorship. In J. Parikka & T. D. Sampson (Eds.), (pp. 229–247). Cresskill: Hampton Press.

Rogers, R. (2009b). *The End of the Virtual: Digital Methods*. Amsterdam University Press.

Rosa, H. (2003). Social Acceleration: Ethical and Political Consequences of a Desynchronized High–Speed Society. *Constellations*, 10(1), 3–33. doi:10.1111/1467-8675.00309

Rosa, H., & Scheuerman, W. E. (Eds.). (2008). *High-Speed Society: Social Acceleration, Power, and Modernity*. University Park: Penn State University Press.

Roseman, E. (2012, January 24). Stop throttling video games, CRTC tells Rogers. Retrieved January 25, 2012, from http://www.moneyville.ca/article/1120828--stop-throttling-video-games-crtc-tells-rogers

Rosen, E., Viswanathan, A., & Callon, R. (2001). RFC 3031: Multiprotocol Label Switching Architecture. Retrieved June 20, 2011, from http://www.ietf.org/rfc/rfc3031.txt

Rosenberg, H., & Feldman, C. S. (2008). *No Time to Think: the Menace of Media Speed and the 24-hour News Cycle*. New York: Continuum.

Russell, A. L. (2006). "Rough Consensus and Running Code" and the Internet-OSI Standards War. *Annals of the History of Computing*, *28*(3), 48–61.

SAGE - Semi Automatic Ground Environment - Part 1/2. (2007). Retrieved from http://www.youtube.com/watch?v=vzf880M9egk&feature=youtube_gdata_player

Saltzer, J. H., Reed, D. P., & Clark, D. D. (1984). End-to-End Arguments in System Design. *ACM Transactions on Computer Systems*, *2*(4), 277–288.

Salus, P. H. (1995). *Casting the Net: From ARPANET to Internet and Beyond*. Boston: Addison-Wesley.

Samuelson, P. (2004). What's at Stake in MGM v. Grokster? *Communications of the ACM*, *47*(2), 15–20.

Sandvig, C. (2006). Shaping Infrastructure and Innovation on the Internet: The End-to-End Network that isn't. In D. Guston (Ed.), (pp. 234–255). Madison: University of Wisconsin Press.

Sandvig, C. (2007). Network Neutrality is the New Common Carriage. *Info: The Journal of Policy, Regulation, and Strategy*, *9*(2/3), 136–147.

Sandvine Inc. (2009). Reply Comments on Public Notice 2008-19 - Review of the Internet traffic management practices of Internet service providers. Retrieved from http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029804.zip

Sandvine Inc. (2010, October 20). Sandvine Internet Report: Average is Not Typical. Retrieved July 21, 2012, from http://www.sandvine.com/news/pr_detail.asp?ID=288

Sandvine Inc. (2011, May 17). Sandvine's Spring 2011 Global Internet Phenomena Report Reveals New Internet Trends. Retrieved July 21, 2012, from http://www.sandvine.com/news/pr_detail.asp?ID=312

Schaffer, S. (1994). Babagge's Intelligence: Calculating Engines and the Factory System. *Critical Inquiry*, *21*(1), 203–227.

Scheuerman, W. E. (2001). Liberal Democracy and the Empire of Speed. *Polity*, *34*(1), 41–67.

Scheuerman, W. E. (2004). *Liberal Democracy and the Social Acceleration of Time*. Baltimore: Johns Hopkins University Press.

Schiesel, S. (2004, February 12). File Sharing's New Face - New York Times. Retrieved July 22, 2012, from http://www.nytimes.com/2004/02/12/technology/file-sharing-s-new-face.html?pagewanted=all&src=pm

Selfridge, O. (1959). Pandemonium: A Paradigm for Learning. *Mechanisation of Thought Processes: Proceedings of a Symposium held at the National Physical Laboratory on 24th, 25th, 26th and 27th November 1958* (pp. 511–529). London: Her Majesty's Stationery Office.

Senft, T. M. (2003). Bulletin-Board Systems. (S. Jones, Ed.)*Encyclopedia of New Media: An Essential Reference to Communication and Technology*. Thousand Oaks: Sage Publications.

Shade, L. R. (1994). Computer networking in Canada: from CAnet to CANARIE. *Canadian Journal of Communication*, *19*(1), 53–69.

Shade, L. R. (1999). Roughing It in the Electronic Bush: Community Networking in Canada. *Canadian Journal of Communication*, *24*(2), 179–198.

Shah, R. C., & Kesan, J. P. (2007). The Privatization of the Internet's Backbone Network. *Journal of Broadcasting & Electronic Media*, *51*(1), 93–109.

Shannon, C. E., & Weaver, W. (1949). *The Mathematical Theory of Communication*. Urbana: University of Illinois Press.

Sharma, S. (2011). The Biopolitical Economy of Time. *Journal of Communication Inquiry*, *35*(4), 439 –444. doi:10.1177/0196859911417999

Sherrington, S. (2011, October 14). DPI Goes Undercover. Retrieved July 22, 2012, from http://www.heavyreading.com/insider/document.asp?doc_id=213442

Shifman, L. (2011). An Anatomy of a YouTube Meme. *New Media & Society*, *14*(2), 187–203. doi:10.1177/1461444811412160

Simon, H. (1971). Designing Organizations for an Information-Rich World. In M. Greenberger (Ed.), *Computers, Communications and the Public Interest* (pp. 37–72). Baltimore: The Johns Hopkins University Press.

Simondon, G. (1992). The Genesis of the Individual. In J. Crary & S. Kwinter (Eds.), *Incorporations* (pp. 297–319). New York: Zone.

Simondon, G. (2009a). The Position of the Problem of Ontogenesis. (G. Flanders, Trans.)*Parrhesia*, *7*, 4–16.

Simondon, G. (2009b). Technical Mentality. (A. De Boever, Trans.)*Parrhesia: A Journal of Critical Philosophy*, (*7*), 17–27.

Sipser, M. (2006). *Introduction to the Theory of Computation* (2nd ed.). Boston: Thomson Course Technology.

Skakov, N. (2012). *The Cinema of Tarkovsky: Labyrinths of Space and Time*. London: I.B.TAURIS.

Smythe, D. W. (1981). *Dependency Road: Communications, Capitalism, Consciousness and Canada*. Norwood, N.J.: Ablex Pub.

Snader, J. C. (2005). *VPNs Illustrated: Tunnels, VPNs, and IPsec* (1st ed.). Boston: Addison-Wesley Professional.

Socolow, M. J. (2007). A Wavelength for Every Network: Synchronous Broadcasting and National Radio in the United States, 1926–1932. *Technology and Culture*, *49*, 89–113. doi:10.1353/tech.2008.0006

Standage, T. (2007). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*. New York: Walker & Company.

Starr, P. (2004). *The Creation of the Media: Political Origins of Modern Communications*. New York: Basic Books.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam Books.

Stevenson, J. H., & Clement, A. (2010). Regulatory Lessons for Internet Traffic Management from. *Global Media Journal - Canadian Edition*, *3*(1), 9–29.

Stiegler, B. (1998). *Technics and Time, 1: The Fault of Epimetheus (Meridian: Crossing Aesthetics)*. Stanford: Stanford University Press.

Stiegler, B. (2010). *For a New Critique of Political Economy*. Malden: Polity.

Stover, C. M. (2010). Network Neutrality: A Thematic Analysis of Policy. *Global Media Journal - Canadian Edition*, *3*(1), *75*–86.

Strangelove, M. (2005). *The Empire of Mind: Digital Piracy and the Anti-capitalist Movement*. (Anonymous, Ed.). Toronto: University of Toronto Press.

Strowger, A. (1891). Automatic Telephone-Exchange. Kansas City, Missouri.

Sunde, P. (n.d.). *Chaosradio: The Pirate Bay*. Chaosradio International. Retrieved from http://chaosradio.ccc.de/cri009.html

Tanenbaum, A. S. (2002). *Computer Networks* (4th ed.). New Jersey: Prentice Hall.

Tay, L. (2009, August 4). Pirate Bay's IPREDator not a place to hide - Security - Technology - News - iTnews.com.au. Retrieved July 7, 2011, from http://www.itnews.com.au/News/151988,pirate-bays-ipredator-not-a-place-to-hide.aspx

Terranova, T. (2004). *Network Culture: Politics for the Information Age*. Ann Arbor: Pluto Press.

Tetzlaff, D. (2000). Yo-Ho-Ho and a Server of Warez: Internet Software Piracy and the New Global Informatiion Economy. In A. Herman & T. Swiss (Eds.), (pp. 99–126). New York: Routledge.

The Internet Infrastructure Foundation. (2010, October 21). Three years of Broadband Check – .SE now launching Broadband Check 2.0 | .SE. Retrieved July 22, 2012, from https://www.iis.se/en/pressmeddelanden/3-ar-med-bredbandskollen-%e2%80%93-nu-lanserar-se-bredbandskollen-2-0

The Pirate Bay. (2011). POwer,Net Secret, Broccoli and KOPIMI. Retrieved from http://thepiratebay.org/torrent/4741944/powr.broccoli-kopimi

Thompson, C. (2005, January). Wired 13.01: The BitTorrent Effect. Retrieved August 2, 2011, from http://www.wired.com/wired/archive/13.01/bittorrent.html

Thompson, E. P. (1967). Time, work-discipline, and industrial capitalism. *Past & Present*, (38), 56–97.

Toscano, A. (2009). Gilbert Simondon. In G. Jones & J. Roffe (Eds.), *Deleuze's Philosophical Lineage* (pp. 380–398). Edinburgh: Edinburgh University Press.

Turner, F. (2006). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

Turner, J. (1986). New Directions in Communications (or Which Way to the Information Age?). *Communications Magazine, IEEE*, *24*(10), 8– 15. doi:10.1109/MCOM.1986.1092946

Valley Jr., G. E. (1985). How the SAGE Development Began. *Annals of the History of Computing*, *7*(3), 196–226.

van Dijck, J. (2009). Users like You? Theorizing Agency in User-Generated Content. *Media, Culture & Society*, *31*(1), 41–58.

Van Schewick, B. (2010). *Internet Architecture and Innovation*. Cambridge: The MIT Press.

Virilio, P. (1995). *The Art of the Motor*. (J. Rose, Trans.) (Original work published in 1993.). Minneapolis: University of Minnesota Press.

Virilio, P. (2004). The Overexposed City. In S. Redhead (Ed.), *The Virilio Reader* (pp. 84–99). New York: Columbia University Press.

Virilio, P. (2006). *Speed & Politics*. (M. Polizzotti, Trans.) (Original work published in 1977.). New York: Semiotext(e).

Wajcman, J. (2008). Life in the Fast Lane? Towards a Sociology of Technology and Time. *The British Journal of Sociology*, *59*(1), 59–77.

Wasik, B. (2009). *And Then There's This: How Stories Live and Die in Viral Culture*. New York: Viking.

Webster, F., & Robins, K. (1989). Plan and Control: Towards a Cultural History of the Information Society. *Theory and Society*, *18*(3), 323–351.

Welzl, M. (2005). *Network Congestion Control: Managing Internet Traffic*. Chichester: John Wiley & Sons, Inc.

Wiener, N. (1948). *Cybernetics or, Control and Communication in the Animal and the Machine*. New York: J. Wiley.

Wiener, N. (1950). *The Human Use of Human Beings*. Cambridge: Houghton Mifflin Company.

Williams, J. (2011). *Gilles Deleuze's Philosophy of Time: A Critical Introduction and Guide*. Edinburgh: Edinburgh University Press.

Williams, R. (1976). *Keywords: A Vocabulary of Culture and Society* (Revised Edition, 1983.). London: Fontana Paperbacks.

Williams, R. (1980). *Culture and Materialism: Selected Essays* (Radical Thinkers Edition, 2005.). London: Verso.

Williams, R. (1990). *Television: Technology and Cultural Form* (Second Edition, 1990. First Edition published in 1974.). New York: Routledge.

Wise, J. M. (1997). *Exploring Technology and Social Space*. Thousand Oaks: Sage Publications.

Wise, J. M. (2005). Assemblage. In C. J. Stivale (Ed.), (pp. 77–87). Montreal: McGill-Queen's University Press.

Wolin, S. (1997). What Time Is It? *Theory & Event*, *1*(1). Retrieved from http://muse.jhu.edu/journals/theory_and_event/v001/1.1wolin.html

Wolin, S. (2004). *Politics and Vision: Continuity and Innovation in Western Political Thought*. Princeton: Princeton University Press.

Wood, D., Stoss, V., Chan-Lizardo, L., Papacostas, G. S., & Stinson, M. E. (1988). Virtual Private Networks. *Private Switching Systems and Networks, 1988., International Conference on* (pp. 132–136). Presented at the Private Switching Systems and Networks, 1988., International Conference on.

Woods, A. (2011, February 18). Canada News: Cyber attack puts Ottawa's security strategy to the test - thestar.com. Retrieved October 27, 2011, from http://www.thestar.com/news/canada/article/940527--hacking-attempt-shows-ottawa-lacking-in-cyber-security

Wouters, P., Hellsten, L., & Leydesdorff, L. (2004). Internet Time and the Reliability of Search Engines. *First Monday*, 9(10). Retrieved from http://www.firstmonday.org/issues/issue9_10/wouters/index.html

Wu, T. (2003a). Network Neutrality, Broadband Discrimination. *Journal on Telecommunication & High Techology Law*, 2, 141–179.

Wu, T. (2003b). When Code Isn't Law. *Virginia Law Review*, 89(4), 104–170.

Wu, T., & Yoo, C. S. (2007). Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate. *Federal Communications Law Journal*, 59(3), 575–592.

Wynne, B. (2007). Public Participation in Science and Technology: Performing and Obscuring a Political–Conceptual Category Mistake. *East Asian Science, Technology and Society: an International Journal*, 1(1), 99–110. doi:10.1007/s12280-007-9004-7

Yates, J. (1989). *Control through Communication: The Rise of System in American Management*. Baltimore: Johns Hopkins University Press.

Zetter, K. (2011, July 11). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History | Threat Level | Wired.com. Retrieved October 27, 2011, from http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1

Zittrain, J. (2008). *The Future of the Internet and How to Stop It*. New Haven: Yale University Press.