The Dialectical Nature of Control Upon Electronic Networks

by

Rawlson O'Neil King, B. J.

A thesis submitted to the Faculty of

Graduate Studies and Research in partial fulfilment

of the requirements for the degree of

Master of Arts

in Mass Communication

Carleton University
OTTAWA, Ontario
December 2006

Your file Votre référence
ISBN: 978-0-494-26952-7
Our file Notre référence
ISBN: 978-0-494-26952-7

Abstract

This thesis examines the imposition of control upon electronic networks. It provides a theoretical review of control and discusses how competing visions of control permeate the design and evolution of communication networks. Drawing upon a notion of duality, this thesis maintains that control is a contested domain that oscillates between open and enclosed models. Open models of control allow for participation and innovation among individuals and small firms, with a lack of restriction. Enclosed models, in contrast, are architectural designs imposed by large communication providers that can limit participation, innovation and interconnection. This thesis investigates how these modalities of control are technologically implemented upon the Internet. Drawing upon arguments by Lessig (1999) and Mansell (1996), it maintains that control is a central component of network design. It examines emerging network control technologies, such as Quality of Control (QoS) and network centralization, and new political debates concerning the neutrality of networks.

Acknowledgements

I am very much indebted to Professor Dwayne Winseck for his invaluable suggestions, patience and input during the development and preparation of this thesis. I also wish to acknowledge the support I have received from the School of Journalism and Communication at Carleton University. Most importantly, I recognize Linda Loraine Angela Grussani who has guided and counseled me for 10 years on virtually every issue in my life. I am proud of her and can never thank her enough for her love and support.

Table of Contents

Chapter 1 Introduction

This thesis examines the dialectical nature of electronic communication networks such as the Internet. It conceives of networks as either open or closed architectures and argues that architecture fundamentally impacts the way that both people and businesses use networks respectively. This thesis describes open and closed architectures and argues that control oscillates between them, encapsulating differing philosophical approaches.

Legal scholar Lawrence Lessig (1999; 2002; 2002a) recognizes that open networks constitute "architectures of innovation" which allows individuals and smaller firms to plug any device or application into the Internet infrastructure with a minimum of restrictions. With the potential for end-users to exercise control, there is no need to go through gatekeepers or bureaucratic processes of economic justification and technical development. Instead, users can simply deploy new applications and devices and make them available to other users to access.

Open networks are guided by an "end-to-end principle" of network architecture design. According to network engineers, the end-to-end principle states that application-level functions should not be incorporated into the core of the network (Saltzer, Reed and Clark, 1998). Instead, applications should only be deployed at the end-points of the communication system. Such architecture allows end-users to circumvent monopolistic control over network resources. Open models of control advocate for wide interconnection and accessible protocols that do not impede

innovation or creativeness. Under this approach, multiple service providers can flourish and all businesses have equal access to network resources in order to develop new products and services. Open architectures allow all users to participate in the usage and deployment of network applications. Due to the emergence of open architectures, the penetration of the Internet has grown exponentially.

In contrast, closed architectures typically attempt to centralize network resources, enact controls on resources that were previously open, and implement regimes of technological design that create closed network environments that restrict what users can and cannot do with different communication technologies.

Improved control over network infrastructure is achieved through the implementation of intelligent network technologies. According to communication scholar Robin Mansell (1993), an intelligent network incorporates new technology into the digital switches or hubs of the network to permit much greater flexibility in providing multiple services to different classes of customers. For Mansell, the new technologies embodied in the intelligent network are vulnerable to manipulation through the exercise of economic and political power made possible largely by institutional arrangements put in place by communication firms seeking to retain or increase market share. The result is that large service providers can exercise a greater amount of control over network resources, while limiting competition by other service providers.

Technological mechanisms employed to achieve greater control under the rubric of intelligent networks include Quality of Service (QoS), which permits greater control over networks by large communication firms that are increasingly utilized for economic

transactions. QoS works to improve control by identifying data traffic types and maintaining the transmission priority of certain types of traffic. It also works to monitor and restrict the actions of users at the end of the network, in direct contradiction to open architectural designs. Greater control is also accomplished through the centralization of servers, applications and other network facilities. Centralization moves network resources from the periphery to its core, allowing service providers to monopolize business service offerings, and limit the use of such applications on the edge of the network.

The consequence of this is that two separate spheres of influence upon networks emerge: one that is dominated by large business to promote their high priority applications and one that is dominated by regular end-users and given less priority. Examining this dichotomy of control; its evolution in network environments from open to closed architectures; and its social impacts, are primary objectives of this thesis. This thesis maintains that control is a contested domain that swings between the open and enclosed models. Under such conditions, electronic networks are interpreted as terrains of social conflict, where differing interests compete. These interests are made up of individuals and innovative firms that leverage open networks for enhanced communication and competition, and by large communication firms and enterprises that wish to use closed networks to enhance their competitive advantage. This thesis sheds light on these divergent interests and examines approaches to control by investigating principles of network engineering and design as proposed by Lessig (1999), philosopher Andrew Feenberg (1995) and Mansell (1996). In terms of design, this thesis draws

strongly upon Mansell's notion of a design principle that states that technology is influenced by both human and organizational intentions.

To understand control as a phenomenon, this research project first examines theoretical conceptualizations of control to demonstrate how traditional communication scholarship has gravitated towards top-down interpretations. Neo-Marxian (Jhally, 1989; Smythe, 1981) and other critical, sociological scholarship (Beniger, 1986; G.T. Marx, 2002) are shown to interpret control as the pejorative imposition of political power, mechanisms of surveillance and social engineering. For these scholars, control is an inexorable or inflexible concept, which imposes inescapable top-down control.

In contrast, newer approaches to control, primarily those outlined by communication scholar Geoff Mulgan (1991), acknowledge control as duality. Rather than an imposed mechanism, Mulgan argues that control is a contested realm, where the struggle for dominance over information technology and resources can be contested from the bottom-up.

He notes that there are two types of control that need to be considered: *exogenous* and *endogenous* control (Mulgan, 1991: 4). Exogenous control is the capacity to exert influence over the environment, systems and individuals outside of a medium. Endogenous control, in contrast, is conceptualized as an internal system for regulating a system itself. The traditional concern with control, in this sense, is only preoccupied with top-down exogenous control. Mulgan however points out that control might also be exerted from the bottom up, or across the system. Traditional concerns

over control, therefore, are likely to ignore substantial portions of any systems' capacity for control (Bates, 1997).

Under Mulgan's conceptualization, the struggle for control over information and communication is actively contested. The social relations of power behind computer-mediated communication are normally associated with: limitations in access; communication competence; commercial interests; the public interest; and public opinion and government action or inaction, all of which constrain the communication capacities of electronic networks. However, communication technologies also contain features that permit agency and action amongst people. Since critical scholars mostly defined communication as asymmetrical information systems or limited two-way communication relationships, information itself is perceived as strictly an instrument of control, supplied from positions of authority to users that are positioned as either consumers, or, as in the case of entertainment and leisure services, audiences. Mulgan's approach to control, in contrast, identifies the potential for true two-way communication and information systems that can be influenced by the audience or general public.

Though this thesis acknowledges two separate models of control, I also argue that control can evolve from openness to enclosure. In specific terms, this thesis looks at communication theorist Robin Mansell's *idealist* and *strategic* models of network evolution and how these models influence network design. Mansell (1993: 18) argues that advances in the technological design of telecommunication networks demonstrate that technology does not encourage a shift from "monopoly to competition, but from monopoly to strategic oligopoly." She observes that though large network operators

typically tout an idealist model, which claims that technology allows for user-driven deployment of innovation, the reality is that the strategic model is normally pursued, reinforcing the control capacity of larger telecommunication firms at the detriment of end-users.

This thesis identifies the implementation of strategic technologies, which includes the use of technological intermediaries such as Quality of Service (QoS) and centralized network resources. It describes the deployment of these network intermediaries and investigates what service providers are implementing them. It also works to juxtapose the technological differences between protocols of enclosure and protocols employed on open networks.

Ultimately, this thesis argues that the implementation of technological intermediaries creates new corporate network environments, characterized by user associations, which are specialized along various dimensions such as geography, price, size, performance, added value, ownership status, access rights, kinds of specialization and extent of internationalization.

The result of this new network configuration is that organizational control is superimposed upon certain classes of network traffic; users; and applications, hence causing the development of a new regulatory framework based upon technology. Under this new framework, closed and open network environments co-exist and network usage is stratified.

Stratification occurs because corporate interests attempt to limit access and control over electronic networks in order to protect the massive investments made in

information and communication technologies and the centrality of networks to advanced capitalist economies. While open networks still exist, this thesis argues that corporate interests increasingly place far greater importance on enclosed "strategic" network architectures that guard against complexity in society and the marketplace. The main reason for this emphasis is due to the growing centrality of networks to economies and the corporate requirement for strategic control over coordinated business processes.

1.1 Centrality of Electronic Networks to Advanced Economies

Electronic networks assume an important economic role since they constitute conduits that support new informational models. Electronic networks have the real-time capability to store, process and manipulate information (Johnston *et al.*, 1995). Such systems therefore facilitate trade in information-based commodities, financial instruments, and in coordinating business activities. Global computer linkages lead to lower costs for conducting business, including those costs associated with transactions, marketing, inventory, distribution and production. Networks also allow increased market share and penetration of new markets through shorter procurement cycles and product customization. As a result, enterprises and commercial network providers consider the entire constellation of electronic networks as strictly a commercial infrastructure, designed mainly to provide a wide range of products and services, and to serve the role of strategic economic investments. As economic investments, networks are intended to maximize returns to investors by offering the use of advanced applications and services to the business community and by extending markets.

Electronic networks have become the backbone of global corporate operations and the key delivery system for supporting large-scale businesses. Networks based upon interoperable standards enable real-time communication and permit access to collective information resources from a myriad of different geographical locations. Sociologist Manuel Castells (1989: 348) identifies these new communication frameworks as a new geography, or "space of flows", in which "the deployment of the functional logic of power-holding organizations in asymmetrical networks of exchange do not depend on the characteristics of any specific locale for the fulfillment of their fundamental goals."

His proposition is that globalization, or the new global economy, is dependent upon new technical processes driven by microelectronics, computing, telecommunication and opti-electronics, which are all bound by an inclusive network logic that connects and integrates dispersed economies. Castells (1996: 136) observes that new technologies and communicative frameworks, especially computer networking, allow core economic activities to be internationalized:

> Advanced computing systems allow new powerful mathematical models to manage complex financial products and to perform transactions at high-speed. Sophisticated telecommunication systems bind financial centers in real time. Online management allows firms to operate on a global basis. Microelectronics-based production makes possible the standardization of components and customization of products through high volume, flexible production. Transnational production networks of goods and services rely on an interactive system of communication, and transmission of information to ensure feedback loops, and to set up co-ordination of decentralized production and distribution.

Evidence of the new, interactive system of communication is apparent through the advent of the Internet, which is a collective formulation of thousands of electronic

networks, and other inter- and intra-organizational networks, central in coordinating real-time economic transactions on a global basis. Collective networks, based upon internetworking technologies, permits heightened control over disparate business operations, creating new financial products and accelerating financial transactions.

According to geographer and political economist David Harvey (1990), the ability to produce new financial products and services and to find new ways of reproducing existing commodities deepens and extends the process of accumulation. The result is an increased reliance upon information and communication frameworks, such as electronic networks, to control and access markets in order to gain competitive advantage (Harvey, 1990: 294-295). Networks have become mechanisms that complement traditional face-to-face public markets with dispersed virtual marketplaces.

The existence of interconnecting electronic networks enable markets to become more extensive, so that work and economic transactions are performed from a variety of locations and structured to operate on a global scale. Networks therefore function as agents of decentralization. They are also central in the co-ordination of transactions between buyers and suppliers worldwide, generating substantial economic benefits in the process. Electronic networks can be extremely efficient marketplaces where buyers and sellers can find each other easily, interact directly, and perform transactions with minimal overhead costs (Castells, 1996: 102). Consequently, networks as systems of commercial activity are an increasingly common institutional structure resulting from the widespread use of telecommunications within advanced capitalist societies.

In the contemporary era, developments in computer communication networks such as the Internet facilitate globalization because they provide the communication pathways central to the circulation of data and information. Such pathways enable the development of financial, consumer and industrial markets. Consequently within the late twentieth-century and beyond, large corporations intensified the construction of networks to implement new economic models. These new models, often referred to as network economies, facilitated the emergence of information marketplaces and intensified international commodity and financial exchange.

The existence of interconnected networks enables markets to become more extensive, rapid and accessible, permitting the unfettered transmission of information as consumer goods (Mosco, 1996). Information within the network economy is hence considered a commodity to be accumulated or exchanged for capital. It becomes so important within the network economy, that it is considered the primary driver that transforms economic production from an industrial to informational mode. This transformation is characterized by the fact that productivity and competitiveness are increasingly based on the generation of new knowledge, and on the access to, and processing of appropriate information.

In 1957, Nobel Prize-winning economist Robert Solow argued that the last half of the twentieth century would be characterized by a new equation in the generation of productivity and thus economic growth (Babe, 1994: 43). Instead of the quantitative addition of capital, labour and raw material typical of the function of productivity growth in both agrarian and industrial economies, the new economy that emerged in

advanced industrial countries since the 1950s increasingly depended on a new econometric equation. This equation would calculate the input of science, technology and the management of information in the production process to determine productivity growth. Economist Fritz Machlup (1962) specifically identifies information and knowledge processing as central to the dynamics of evolving advanced capitalist economies. Previous to Machlup's analysis, macroeconomic analysis only assumed a threefold division to the economy between agricultural, manufacturing and service sectors. However, in calculating that a substantial proportion of U.S. economic output and employment are dedicated to the knowledge industries, Machlup advances the argument that a fourth sector of the economy exists, one based upon informational and communicatory activities and products (Babe, 1994: 43).

In the late 1970s, economist Marc Porat (1977) advanced Machlup's theory by pronouncing that the United States had developed into a "information economy". While Machlup (1962) estimated that 29 percent of U.S. output was dedicated to the information sector in 1958, Porat (1977) estimated that by 1967, the knowledge industries had accounted for nearly half of the American gross domestic product (GDP).

Economists argue that advanced capitalist societies have become increasingly characterized by the ever-growing role of symbols in the organization of production and in the enhancement of productivity. Such societies are described as shifting from material production to information-processing activities, in terms of the proportion of the population employed in such activities. Accordingly, these theorists argue that information itself has become the transforming resource of economic organization.

Post-industrialists such as Daniel Bell (1973) note that new intellectual technologies, primarily the computer and its peripherals, are dramatically discontinuous with earlier systems of information processing. For Bell, the "post-industrial society" brakes with and transcends elemental relations including, most crucially, the opposition between capital and labour, which shaped its industrial antecedent. Under such conditions, knowledge and technology supplants capital and labour as the decisive factor of production. Communication theorists have therefore described a "post-industrial" (Bell, 1973) or "information society" (Machlup, 1962) as an era of societal development that is dominated by an "informational mode" of production, or a digital or network economy (Castells, 1996), or by the "informatization" of socio-economic processes (Harvey, 1990). Many other scholars maintain that new technologies ushered in many societal transformations since 1950, as indicated in the table below (Beniger, 1986: 4).

Year	**Transformation**	**Sources**
1950	Lonely crowd	(Riseman, 1950)
	Posthistoric man	(Seidenberg, 1950)
1953	Organizational revolution	(Boulding, 1953)
1956	Organizational man	(Whye, 1956)
1957	New social class	(Djilas, 1957); (Gouldner, 1979)
1958	Meritocracy	(Young, 1958)
1959	Educational revolution	(Drucker, 1959)
	Postcapitalist society	(Dahrendofr, 1959)
1960	End of ideology	(Bell, 1960)
	Postmaturity economy	(Rostow, 1960)
1961	Industry society	(Aron, 1961;1966)
1962	Computer revolution	(Berkeley, 1962); (Tomeski, 1970); (Hawkes, 1971)

1963	New working class	(Mallet, 1963); (Gintis, 1970); (Gallie, 1978)
	Postbourgeois society	(Lichthiem, 1963)
1964	Global village	(McLuhan, 1964)
	Managerial capitalism	(Marris, 1964)
	One-dimensional man	(Marcuse, 1964)
	Service class society	(Dahrendorf, 1964)
	Technological society	(Ellul, 1964)
1967	New industrial state	(Galbraith, 1967)
	Scientific-technological revolution	(Richta, 1967); (Daglish, 1972)
1968	Dual economy	(Averitt, 1968)
	Neocapitalism	(Gorz, 1968)
	Postmodern society	(Etzioni, 1968); (Breed, 1971)
	Technocracy	(Maynaud, 1968)
1969	Age of discontinuity	(Drucker, 1969)
	Postcollectivist society	(Beer, 1969)
	Postideological society	(Feurer, 1969)
	Knowledge economy	(Drucker, 1969)
1970	Computerized society	(Martin and Norman, 1970)
	Personal society	(Halmos, 1970)
	Posteconomic society	(Kahn, 1970)
	Postliberal age	(Vickers, 1970)
1971	Postindustrial society	(Touraine, 1971); (Bell, 1973)
	Superindustrial society	(Toffler, 1971)
1972	Posttraditional society	(Eisenstadt, 1972)
	World without borders	(Brown, 1972)
1973	New service society	(Lewis, 1973)
1974	Consumer vanguard	(Gartner and Riessman, 1974)
	Information revolution	(Lamberton, 1974)
1975	Communications age	(Phillips, 1975)
	Mediacracy	(Phillips, 1975)
	Third industry revolution	(Stine 1975); (Stonier, 1979)
1976	Industrial-technological society	(Ionesu, 1976)
1977	Electronics revolution	(Evans, 1977)
	Information economy	(Porat, 1977)
1978	Anticipatory democracy	(Bezold, 1978)
	Network nation	(Hiltz and Turoff, 1978)
	Telematic society	(Nora and Mic, 1978); (Martin, 1981)
	Wired society	(Martin, 1978)
1979	Collapse of work	(Jenkins and Sherman, 1979)
	Computer age	(Dertouzous and Moses, 1979)
	Credential society	(Collins, 1979)
	Micro millennium	(Evans, 1979)
1980	Micro revolution	(Large, 1980, 1984); (Laurie, 1981)
	Microelectronics revolution	(Forester, 1980)
	Third wave	(Toffler, 1980)
1981	Information society	(Martin and Butler, 1981)
	Network marketplace	(Dordick *et al.*, 1981)
1982	Communication revolution	(Williams, 1982)
	Information age	(Dizard, 1982)
1984	Second industrial divide	(Piore and Sable, 1984)

Table 1.1.1 – Modern Societal Transformations Identified Since 1950 (Beniger, 1986: 4)

While these scholars might be divided on whether the above-mentioned modern social transformations were an elemental, disruptive break with the past or part of an evolutionary process, the one consistent factor is that the kind of changes they outline have been influenced by dramatic increases in knowledge and technology since the middle-to-late twentieth century. As communication scholar Frank Webster (in Alberts and Papp, 1997: 52) notes:

> The most common definition of the information society emphasizes spectacular technological innovation. The key idea is that breakthroughs in information processing, storage, and transmission have led to the application of information technologies (IT) in virtually all corners of society. The major concern is the astonishing reductions in the costs of computers, their prodigious increases in power, and their consequent application anywhere and everywhere.

The term "information society" is therefore widely used shorthand for complex social, economic and institutional changes related to the proliferation of information and communication technologies that lead to profound changes in capitalism and the wide adoption of networks. According to sociologists Scott Lash and John Urry (1994), capitalism from the late twentieth century onward has entered into a new "disorganized" stage, in which the networked flows of capital, labour, commodities, information and images across time and space becomes axial.

According to communication scholar Jan van Dijk (1999), capitalist societies are increasingly organized in network structures, fulfilling vital economic functions in progressively complicated systems. As a result, the development of social structures becomes increasingly influenced by technological infrastructure. In fact sociologist Barry Wellman (2001) theorizes that electronic networks are inherently social networks themselves, since they link people, organizations and knowledge. A social network is

traditionally defined as a social structure between actors, mostly individuals or organizations. Since social networks are acknowledged to be subject to the exigencies of control, so to by extension are electronic networks.

Networks create opportunities for businesses to develop new mechanisms of control through co-ordination. Co-ordination is defined as "the process of managing dependencies between activities" (Cited in Malhotra, 1996). Business professor Thomas Malone (1997) argues that because electronic networks reduce the cost of coordinating business processes between firms, networks allow firms to conduct more transactions across organizational boundaries and to become virtual, and by extension global. A number of authors have even followed in hypothesizing that by lowering co-ordination costs, electronic networks enable "virtual organizations" (Ahuja and Carley, 1998; Olson, Malone and Smith, 2001). They argue that both governance and co-ordination costs lead to the use of electronic networks by firms to outsource more elements of the production process.

Under the theory of co-ordination, transnational corporations change from being vertically integrated to becoming so disintegrated as to transform into horizontal organizations, or conceptually into social networks themselves (Malone, 1997). Castells (1996) argues that the high value placed on speed and adaptability is of tremendous importance to maintain co-ordination.

He thus advances the idea that even though transnational corporations continue to exist they have changed dramatically. Many organizations are no longer centrally planned and operated, or self-contained and self-sufficient. Instead, enterprises devolve

power to those with access to a network of self-programmed, self-directed units based on decentralization, participation and co-ordination. In this way the globalization of competition dissolves the large corporation into a web of multi-directional social networks. These conceptual networks are places where strategic alliances are made and abandoned depending on particular circumstances and participants. Electronic networks are the technical form assumed by these conceptual networks to facilitate business relationships and economic transactions.

1.2 Financial Investments in Electronic Networks

Networks are locations where a tremendous amount of wealth and investment becomes concentrated. Consequently, information and communication technologies are designed to provide a wide array of products and services to accommodate business requirements (Gutstein, 1999; Schiller, 1999). In order to support the massive flows of goods, services, foreign currency and securities over networks, billions of dollars are being invested in supporting telecommunication and computer network infrastructure.

In 2004, all spending on telecommunication equipment and services in the United States totaled more than $95 billion U.S. (Telecommunications Industry Association, 2004). Business spending on such equipment was particularly rampant, as leading U.S. companies sought to integrate networks in core activities of production, marketing and administration.

In 1996, for example, more than one-third of all U.S. spending on capital facilities for telecommunication occurred outside the sphere of common carrier

investment, and the resulting electronic networks, of which there were thousands, grew by 30 to 40 percent per year (Cairncross, 1995). According to the Cahners In-Stat Group (2000), by September 2000 the majority of large U.S. firms were investing as much as 20 percent of total information technology expenditure dollars on information technology (IT) services, personnel and solutions.

The mobilization by enterprise to deploy and utilize networking technology resulted in huge investments in information technology. Computers, telecommunication equipment and software accounted for nearly 12 percent of U.S. capital stock by the mid-1990s (Woodall, 1995). The share claimed by the information technology sector in the U.S. gross domestic product increased disproportionately, from 4.9 percent in 1986 to an estimated 8.2 percent in 1998 (U.S. Department of Commerce, 1998).

From 1996 to 2000 the IT sector in the United States accounted on average for seven percent of GDP and grew 21 percent annually, accounting for 28 percent of overall real economic growth. U.S. businesses are IT consumers, who spent $258 billion (U.S.) on IT goods and services in 2000 (U.S. Department of Commerce, 2003).

Total American spending on information and communication technologies (ICT) had increased almost 70 percent from 1992, to almost $813 billion (U.S.) in 2001 (Information Technology Association of America, 2003). Between 1993 and 2001, ICT in the U.S. had achieved a compound annual growth rate of 6.7 percent, compared to 7.6 percent for all global economies (Information Technology Association of America, 2003). In customer terms in the United States, at 6.64 percent, the financial services industry spent the greatest share of total 2002 revenues on ICT, followed by

telecommunication (6.4 percent), banking (5.37 percent), and the information technology industry itself at 5.13 percent (Information Technology Association of America, 2003).

In Canada, the information and communication sector also emerged as a significant component of the national economy. In 1995, it accounted for 7.6 percent of Canada's gross domestic product (GDP) at factor cost, up from 5.5 percent in 1990 (Statistics Canada, 2003). Trade in information technology services almost tripled from $515 million (Canadian) in 1990 to $1.5 billion (Canadian) in 1995 (Statistics Canada, 2003). Business and government spending on ICT increased from $3.3 billion (Canadian) in 1982 to over $30 billion (Canadian) in 1998 (Statistics Canada, 1999). In 2002, the ICT sector contributed $58.7 billion (Canadian) to Canada's GDP, accounting for 7.1 percent of business sector GDP, and six percent of total economy GDP (Statistics Canada, 2004). ICT sector growth over the 1997-2002 period was 79.3 percent, substantially higher than business sector growth and more than four times the growth of the total economy (Statistics Canada, 2004).

A comparative analysis of software and ICT investments from 1990 to 2000 in Canada and the United States reveals a continuing growth pattern in business spending, as a percentage of non-residential gross fixed capital, as illustrated in the following chart derived from data from the Organisation for Economic Co-operation and Development (OECD, 2002).

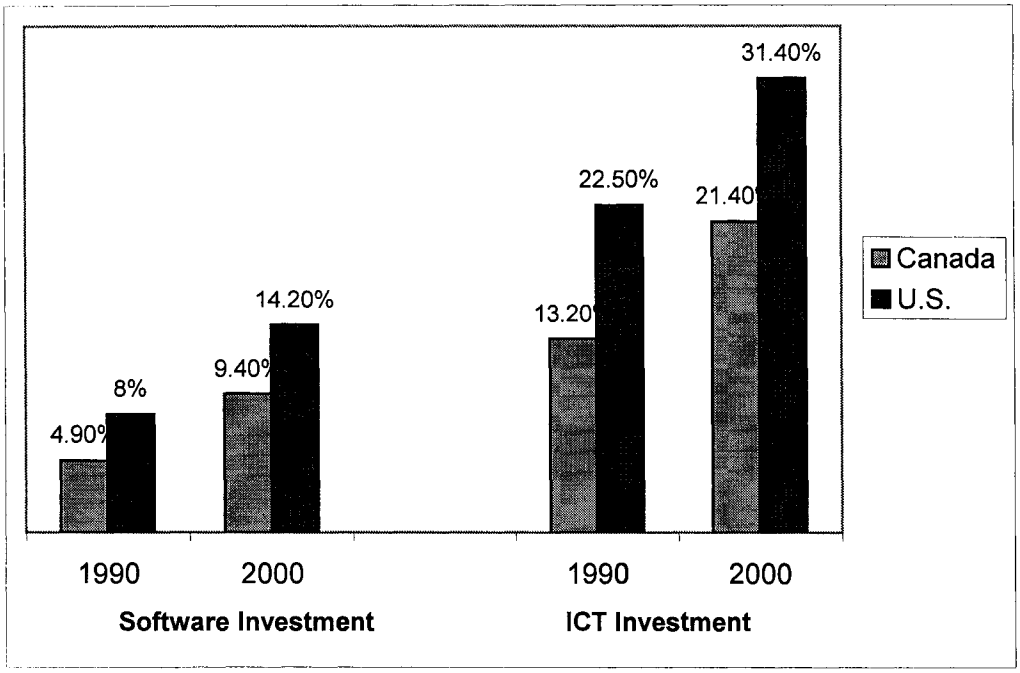

Chart 1.2.1 – Comparative Investments in Software and Information and Communication Technologies in Canada and the United States (OECD, 2002).

In absolute terms and as a proportion of total capital investment, network applications and associated infrastructure also occasioned a spectacular increase in capital expenditures in both Canada and the United States. In Canada, up to five percent of large business total expenditures in 1994 were on telecommunication services, according to Industry Canada. The government department noted that a study of business use of telecommunication services in Canada during 1994 revealed that about half of all large business spent over $10,000 (Canadian) per month on such services (Winseck, 1997: 231). A significant number of large Canadian computer firms, 13 percent, also had bills in excess of $50,000 (Canadian) (Winseck, 1997: 231).

Canada further experienced fast growth in high-speed or "broadband" network services that enables high-speed, two-way transmission of voice, data and multimedia communications. In 2002, most private sector enterprises using the Internet did so through broadband. According to Statistics Canada (2003), 58.4 percent of businesses used it. The number of companies using the Internet via broadband connections increased to approximately 75 percent in 2004, up from 48 percent in 2001, according to a Statistics Canada (2004) study, which examined the impact of the Internet on enterprises. In addition, the 2004 study concluded that 27 percent of companies with broadband connections deployed an internal Web site for their employees.

In the United States, large businesses also placed emphasis on new network services. An estimated nine-tenths of Fortune 500 companies launched intranets, or internal electronic corporate networks in 1997, at a cost of billions of dollars (Schiller, 1999: 17). Market research estimated that global spending on business applications would grow to $131 billion (U.S.) by 2006, continuing the historical trend of increased expenditure on ICT (Forrester Research, 2002). These investments demonstrated that as high-speed, electronic networks such as the Internet became more active and pervasive within the corporate sector, the demand for business applications also grew considerably.

Additional statistics reveal that the largest investments were poured into the expansion of financial networks. For example, the 10 largest U.S. investment banks spent $17 billion (U.S.) on new technologies, amounting to more than $400,000 (U.S.) per employee in 1995 alone (Stalder, 1997). Between 1980 and 2000, such massive

expenditures transformed the financial markets from a relatively peripheral, support phenomenon into the central event of the mainstream economy (Stalder, 1997). These investments led to the automation of financial markets, which in turn dramatically increased the volume of money and transactions. By the mid-1990s, approximately half a million people worldwide worked in financial markets, managing the circulation of more than $1.5 trillion (U.S.) per day (Stalder, 1997). By far, the largest single market was the foreign currency exchange (forex), which amounted in 2002 to more than $1.3 trillion (U.S.) per day (Mathews, 1997). During the 1980s, forex transactions were 10 times larger than total world trade, and in the early 1990s it was 60 times larger (U.S. Department of Treasury, 2000). The use of networks allowed for the improved circulation and acceleration of this capital in ever expanding marketplaces without material friction.

As markets obtained the potential to grow beyond the limitations of time and space within the context of electronic networks, more money became concentrated there. The result was that capitalist markets deepened along with opportunities to make more money, thereby increasing the incentive to deploy more advanced networking technologies.

The tightening link between wealth and communication networks motivated enterprises to impose greater mechanisms of control in order to protect: i) their investments; ii) systems of financial exchange; and iii) the co-ordination of their customers' business activities. Consequently, larger service providers actively moved to

impose a new closed architecture: the intelligent network in order to instill corporate dominance over the network infrastructure.

This thesis examines the evolution towards such a closed architecture and the technologies required to impose it. It also outlines theoretical conceptualizations of control in order to develop a better understanding of the imposition of control mechanisms upon electronic networks.

Chapter 2 Theoretical Conceptualizations of Control

Understanding theoretical conceptualizations of control is key to understanding the impact and the imposition of control technologies upon electronic networks. Control in this thesis is defined as a process that brings about adherence to a goal or objective through the exercise of power or authority (Clemmons and Simon, 2001). In the context of information and communication technologies, control traditionally is viewed as the ability of outside organizations to manipulate a communication system in a purposive manner, in order to direct the system's effects (Pfeffer and Salancik, 1978). Control therefore refers to the basic questions of what degree of control is permitted or encouraged by the structure of a communication system and society, and who is permitted that control (Bates, 1997).

Control is consequently observed as a top-down, imposed mechanism. This chapter reviews the conceptualization of control by neo-Marxists, the Frankfurt School and contemporary critical scholars. It demonstrates that such approaches tend to often interpret control as simply the pejorative imposition of political power, mechanisms of surveillance, and social engineering. The chapter then outlines Geoff Mulgan's interpretation of control and Robin Mansell's idealist and strategic models of advanced network development. Both Mulgan and Mansell view control as a duality. Instead of simply being imposed, they both argue that control is a contested domain, where the struggle for control over information and communication technologies is actively contested from the bottom-up. Under such an interpretation, control is seen as a multi-

faceted phenomenon, rather than an inflexible implementation of surveillance and ideology.

2.1 Neo-Marxist Conceptions of Control

Neo-Marxist conceptions of control stem from a set of perspectives concerned with: i) issues of ideology and ii) and capitalist ownership over the means of production. Sociologist John B. Thompson (1990: 56) defines the concept of ideology as a means to establish and sustain relations of domination and a set of beliefs or values. Though Marx himself did not directly address the notion of communication technologies as control mechanisms *per se*, he did focus on the ability of a dominant, capitalist class to control social institutions and to impose a specific ideology. According to Marxist theory, capitalism is characterized by power and rewards being increasingly concentrated in the hands of those who own the means of production at the expense of the much larger group of people who possess only their own labour power, which they sell in exchange for wages. In this context, according to contemporary neo-Marxian scholars, the economic system reproduces itself to survive through gaining the consent of the dominated through ideology circulated by information and communication technologies. Media, as a result, functions as an instrument for the manufacture and circulation of a dominant ideology and consciousness, which reflects the class interest of its capitalist owners. According to communication theorist Herbert Schiller (1969; 1973), mass media and communication technology is closely tied to the centres of political and economic power. Because of

these ties, they often fall short in their most crucial roles of providing a democratic forum and acting as the watchdog of powerful interests.

Communication scholar Sut Jhally (1989) defines the media as a part of the "consciousness industry", constituted by ideological institutions designed to reify the control of the capitalist class. Jhally (1989) also describes media as mechanisms that facilitate the "industrialization of culture". This approach highlights the commodification of culture under capitalism and its transformation into products and services that are bought and sold in the marketplace. Culture within this approach is no longer seen as an ideological tool that attempts to strengthen ideas, but rather as "part of material production ... subject to the same laws of economic production as other industrial spheres" (Jhally, 1989: 73). From this approach, culture is seen as a commodity in which its exchange value subordinates its use value. According to communication theorist Dallas Smythe (1981), though people generally think the purpose of mass media is to serve them with information or entertainment, those in control of the media know their primary function is to sell audiences to advertisers. As a result, the audience itself actually constitutes a commodity. Marxian-inspired communication studies therefore concentrate almost exclusively on issues of ownership and control.

Such a viewpoint is a logical extension of Marxian thought. Marx emphasized the importance of information and its role concerning the accumulation of capital in a dynamic economic system and its implication for society. He made frequent reference to the role of communications in the evolution of capital within *Grundrisse, Outlines for a Critique of Political Economy.*

Marx (1858: 501) asserted that:

> the more production comes to rest on exchange value, hence on exchange, the more important do the physical conditions of exchange – the means of communication and transport – become for the cost of circulation. Capital by its nature drives beyond every spatial barrier. Thus the creation of the physical condition of exchange – of the means of communication and transport – the annihilation of space by time – becomes an extraordinary necessity for it.

Marx often drew attention to the fact that improvements in the means of communication facilitated competition among workers in different localities and turned local competition into a national affair. He argued that the opportunities created by the development of transportation and communication tended to drive capitalism in the direction of even more remote markets until a world market is reached. Marx (1858: 161) even predicted the development of information marketplaces:

> Institutions emerge whereby each individual can acquire information about the activity of all others and attempt to adjust his own accordingly, e.g., lists of current prices, rates of exchange, interconnections between those active in commerce through the mails, telegraphs, etc. (the means of communication of course grow at the same time). This means that, although the total supply and demand are independent of the actions of each individual, everyone attempts to inform himself about them, and this knowledge then reacts back in practice on the total supply and demand.

For Marx, the crucial motive behind the capitalist development of communications was to shorten the circulation time of commodities and extend them. Communication was therefore a "means of production" that constituted part of the infrastructure of capitalism.

Concerning ideology, Marx argued that through the economic control of the factors of production and persuasion, the dominant class was able to effectively portray their own particular view of the world. The ability to control what amounted to the

systems for transmitting ideology (i.e., communication systems) was therefore seen as being crucial to the maintenance of power in a society (Bates, 1997). Within the context of the capitalist state, the dominant class would employ indoctrination as a means of control and use communication technologies as its conduit. Marketing, advertising and public relations would be employed, using mass communications to aid the interests of the business elite. Information would also be restricted, or rationalized, so that the majority is not provided the information necessary to make rational decisions about social or economic issues. Media and information technology under the Marxist interpretation would therefore be used to obtain societal consent.

The Marxian notion of *hegemony*, as advanced by Antonio Gramsci (1971), espouses that the ruling class exerts dominance over others by obtaining the consent of subordinate classes, rather than resorting to direct coercion. A major component of Marxian thought, hegemony assists in offering a historical and materialist analysis of the relationship of class, which heavily relies upon modes of production, capitalism and the role of class struggle in a changing society.

In terms of a capitalist society, hegemony assists in keeping labour subjugated to capital by utilizing communication systems to further capitalist goals. Neo-Marxist scholarship recognizes the use of telecommunications and information systems to reify existing power structures. Fiske (1996: 217), in his observations on Marxist theory, notes that "communication and information technology does not merely circulate discourse and make it available for analysts, it also produces knowledge and power." Communication technologies under such a model ensure conformity with the accepted cultural,

economical and political norms of the dominant society. Accordingly, elites could "focus on communication technology both as ways of engaging in discourse struggles, and, through their surveillance capability, as ways of producing a particular form of social knowledge and thus of exerting power." (Fiske, 1996: 217)

Power, whether perceived or unacknowledged is free to determine the contents, structure, and procedure of information systems. Science and expertise become the ontological and epistemological servants of powers. Information systems further reify these relations by adopting "expert" standards. The standards imposed by power persist despite intentions to the contrary because the systems do not mandate space for recursive dialogue. Challenge and contest, from whatever source, is marginalized. Information is therefore defined as that which instructs, so despite efforts to the contrary, most information systems are designed as transmission systems, not participation systems. As a result, many neo-Marxist perspectives mainly interpret communication systems under capitalist conditions as systems of indoctrination.

Media and information technology however do have the capacity to liberate humanity from ideological restraint. Such a capacity, according to traditional Marxian theory, is dependent upon how the technology is applied. If information and communication technology is utilized to promote socialist goals, then it is perceived as using its latent, positive potential. Under Marxian theory, science and technology is believed to be a progressive force, if applied for communal rather than for capitalist benefit. Information and communication technologies, under a traditional Marxist

interpretation, therefore, serve as a simple conduit to transmit ideology, whether socialist (liberating) or capitalist (domineering).

2.2 The Frankfurt School's Conceptions of Control

Developing Marx's view that the dominant class in society not only owns the means of material production, but also controls the production of the society's dominant ideas and values (dominant ideology), the Frankfurt School specifically examined the industrialization of mass-produced culture and the economic imperatives behind what it dubbed the culture industries. They reiterated the fundamental Marxist argument that the dominant class exerted direct control over the major communication systems in capitalist societies, and used that control to subvert or contain critical or antithetical perspectives or beliefs (Adorno and Horkheimer, 1972).

As in hegemony theory, this external control was accomplished in part through the commodification of culture and media messages (i.e., through the exertion of internal control over content). The Frankfurt School therefore interpreted the products of the culture industries as providing the ideological "legitimation" of existing capitalist societies, and was the first to recognize the importance of the culture industries as significant agents of socialization. Thus, revisionist Marxist theories were developed by the Frankfurt School to progress typical Marxist thought beyond its rather mechanistic materialism and economic determinism, to include specific consideration of culture as a vehicle of ideology, as well as a concurrent critique of science and technology as tools of social domination within the capitalist system.

Unlike traditional Marxian theorists, the Frankfurt School did not envision science and technology as progressive measures, which had the potential to be used for liberation from the dominance of capital. On the contrary, German philosophers Theodor Adorno and Max Horkheimer (1972) argued that the pursuit of science and technologies by modern societies led to mechanisms of enhanced technical control. Technology to them was a totalitarian tool or a seamless system in which resistance to the status quo was near impossible. Technology, as interpreted by the Frankfurt School, would function to reify instrumental reason.

Instrumental reason is used to describe the organizational principles of social formation, the value orientations of the personality, and the meaning structures of a culture. As defined by Adorno and Horkheimer (1972), it is a mechanism that seeks to transform experiential reality into an experimental one. Under such conditions, reason becomes divorced from morality and reality is made subservient to a rationality that can be reduced to a set of variables or a collection of figures, which gives primacy to statistical and laboratory reality over the personal, social, communal and cultural realities that had abounded in past, pre-modern societies. Instrumental reason fosters the notion that the means by which social and political development is sought are separate from its ends. As a result, reason becomes divided from moral direction and ultimately leads to the destruction of nature, the rise of bureaucratic capitalism, and the reduction of human beings to objects of manipulation.

Adorno and Horkheimer (1972) noted that modern societies were trapped in a paradox, in that they adopted reason, science and technology in order to free themselves

from the bonds of tradition, philosophy and religion, but became trapped by the role of science, which eventually would be touted as the only form of legitimate knowledge. Consequently, modernity reverted to its own tradition of a single truth. But instead of embracing dogmatic religious beliefs, modernity fervently constructed its own dogmatic edifice around science. Adorno and Horkheimer (1972) identified the irony of this paradox and entitled it the "dialectic of Enlightenment." They disdained the elevation of science and the disassociation of humanity from all-encompassing moral systems. Pre-modern cultures approached reality not just in epistemological terms, but also experientially. Modernity however applied force in the form of instrumental reason to break this experiential and relational bond.

Unlike Marxian theory, where *praxis* could be achieved in order to pursue human liberation, the Frankfurt School argued that resistance to domination, *viz.* instrumental reason, was not possible. For the Frankfurt School, humanity in its totality was subject to instrumental reason, and technology was just another one of its variants. Technology under the conditions of modernity worked to continually purify reason into instrumental form. Since reason is purified, so too are the operating environments in which reason functions. A functional object of reason is information. The unfettered use of instrumental reason therefore requires an arena of pure information. The more information is separated from its social and natural contexts, the greater the operational scope of instrumental reason.

Information and communication technologies within such an interpretation would be considered mechanical implementations of instrumental reason (Adorno and

Horkheimer, 1972). Such technologies store, transmit, and manipulate refined information, thereby functioning as information filters. As these technologies proliferate, they create widening zones of refined information, thus expanding the operational scope of all forms of instrumental reason. Within this scope, information and communication technologies are powerful devices for control.

Philosopher Herbert Marcuse (1991), elaborating on the assertions of Adorno and Horkheimer (1972), wrote that "technology serves to institute new, more effective, and more pleasant forms of social control and cohesion" (Marcuse, 1991: xlvii) and that "the technological society is a system of domination which operates already in the concept and construction of techniques" (Marcuse, 1991: xlviii).

Marcuse mirrored the rather bleak perspective of Adorno and Horkheimer; namely, that resistance under this technological regime is near impossible, as evidenced in his statement that, "[i]n the medium of technology: culture, politics, and the economy merge into an omnipresent system which swallows up or repulses all alternatives" (Marcuse, 1991: xlviii). For Marcuse, along with others in the Frankfurt School, communication technology aided systems of social and economic repression.

2.3 Technocracy and Inflexible Regimes of Control

In terms of Marxist scholarship, control over media and ideas are chiefly seen as a means to exercise control over consciousness and obtain consent. The Frankfurt School interpreted media as mechanisms that support totalitarian domination over humanity and nature. For modern sociologists and communication scholars, media technologies are

tools for implementing control over human agency by large organizations in order to further economic or bureaucratic interests. By and large, technology is seen as inflexible mechanisms that impose institutional power.

The technocracy thesis, as described by philosopher Andrew Feenberg (1995), holds that technology is used to consolidate and legitimate an expanding system of hierarchical control. Feenberg (1995: 94) notes that: "Technocracy results from the systematic, long-term selection of those technical alternatives that favor hierarchical control. Devices that can be purchased and introduced at strategic times and places can also be used to transform the normative structures of organizations through technical delegations that embody a new normative consensus in the apparently unchallengeable medium of technical advance." As a consequence, organizations are encountered at every turn attempting to resolve normative disputes through technologies that reinforce their power and legitimacy. To the extent that such organizations grow, the technocracy thesis gains plausibility, justifying the dystopian projections of the dialectic of Enlightenment (Feenberg, 1995).

Contemporary sociologists note that with greater operational autonomy, the influence of organizations become more pervasive. The result is that specialized internal functions of institutions such as workplaces or prisons become general features and even models for social life. Control becomes more integrated into daily living as organizations such as enterprises and governments employ technology to exercise greater top-down hierarchical control. As such, technologies are interpreted as mechanisms of inflexible control by many modern sociologists. Communication technologies are employed as new

mechanisms of inflexible control by: defining new locales, creating new modes of co-ordination, implementing new industrial management techniques, and by developing new systems of classification and observation.

For sociologist Anthony Giddens (1985), *locales* are primarily defined in terms of proximity and co-presence, and electronic media are primarily instruments that facilitate "time-space distanciation" or the integration of distant locales. The integration of distant locales means that disparate units within an organization can co-ordinate their operations on a worldwide scale. In effect, enterprises are able to decentralize their operations, but concurrently retain control through the use of information and communication technologies such as electronic networks. Technology is therefore used as a control mechanism to benefit global business concerns and address the complexity of new advanced industrial societies, based upon information. Its major role is to impose technical controls over corporate processes.

Communication professor James R. Beniger (1986) makes the extended claim that information and communication technologies are also reciprocally subject to inexorable or inflexible regimes of control itself. Through critical scholarship, he traces the intertwined development of technical control from the Industrial Revolution. His theoretical approach emphasizes that control is inseparable from information processes and reciprocal communication "because both the activities of information processing and communication are inseparable components of the control function, a society's ability to maintain control – at all levels from interpersonal to international relations – will be

directly proportional to the development of its information technologies." (Cited in Beniger, 1986: 8)

Beniger (1986: 8) maintains that communication and control are inseparable because two-way interaction of communication and feedback between controller and controlled is central to cybernetics, or the science of communication and control in both animal, human and machine.

He argues that a revolution in control emerged in the second half of the nineteenth century when existing technologies for information processing and communication were not capable of handling the increases in commodity flows generated by mass production and new modes of transportation. Beniger (1986) notes that a control revolution developed in response to problems arising out of advanced industrialization: a mounting crisis of control at the most aggregate level of national and international systems, levels that had little practical relevance before the mass production, distribution and consumption of factory goods.

The response to this crisis amounted to a revolution in societal control. Initially, this control was in the form of bureaucracy, but after the Second World War, it shifted toward computer technology. As Beniger (1992) writes,

> [The] complex and interrelated sequences of rapid change in the technological and economic arrangements by which information is collected, stored, processed, and communicated has come to be known as the Control Revolution. Its ultimate cause was the Industrial Revolution, which dramatically speeded up the material processing systems of developing societies ... thereby precipitating a spreading crisis in control.

> Just as the Industrial Revolution marked a historical discontinuity in the ability to harness energy, the Control Revolution marked a similarly dramatic leap – by means of countless innovations in information and communication technologies – in the ability to harness information for control.

The continual refinement of information and communication technologies under such conditions meant that concurrent refinement of control mechanisms also took place. The result was that society exceedingly became subject to the exigencies of technical control.

Indeed, the noted sociologist Gary T. Marx (2002) argues that science-based technology was increasingly utilized for rule enforcement in society. As a result, a highly "engineered society" emerged based upon an ethos of rationalization which sought as its end-goal to exercise control over business processes and human behaviour. Examples include video and audio surveillance, heat, light, motion, sound and olfactory sensors, electronic tagging of consumer items, animals and humans, biometric access codes, drug testing, DNA analysis, and especially, the use of computer techniques employing electronic networking, which include: expert systems, matching and profiling, data mining, mapping, simulation and electronic network analysis and surveillance (Marx, 2002: 9).

For G. T. Marx (2002), the technological nature of control was key. He noted that control involved ever more integrated information-sharing networks, which blurred many traditional, institutional and organizational bodies (e.g., within and between agencies and levels of government, banks, insurance, health care, education, work, telecommunications, sales and marketing organizations). He found that technical controls were capital-intensive rather than labour-intensive and as a result the cost of

control per unit of information had decreased. More objects and areas within social life were subjected to inspection and control and there was a broadening from the traditional targeting of a specific suspect, to categorical suspicion of individuals, networks, and organizations (Marx, 2002: 9).

According to G. T. Marx (2001: 15507):

> Control has also become more intensive, probing deeply beneath protective surfaces. Many contemporary controls transcend boundaries of distance, darkness, physical barriers and times – factors which traditionally protected liberty, as well as malfeasance. Data can be easily stored, retrieved, combined (from different places and in different forms such as visual, auditory, print and numerical), analyzed and communicated. Control may be remote and deterritorialized, with buffers between controllers and those controlled. Control and knowledge of other's behaviour are no longer restricted to what the senses directly reveal through interaction, nor to a bounded physical place.

For G. T. Marx (2001; 2002), the advent of information and communication technologies, especially electronic networks permitted control to become pervasive. With the wide deployment of networks throughout workplaces and homes, the technical means of control greatly propagated throughout and saturated modern societies, thereby colonizing and documenting ever more areas of social life. Information technology, and electronic networks in particular, acted as corporate mechanisms of domination. According to this school of thought, the roots of contemporary social control lay in the development of large organizations using standardized control technologies to implement systems of constant surveillance and control.

Philosopher Michel Foucault (1977) developed a theory of surveillance that focused on aspects of power, the accumulation of information, and the direct supervision of subordinates. He considered communication technologies as components of a

"panoptic machine" that ensured that individuals were seen, but were not aware that they were seen or were objects of information rather than a subject of communication. The panoptic machine, according to Foucault (1977: 249) is "at once surveillance and observation, security and knowledge, individualization and totalization, isolation and transparency." Accordingly, it is an integrated system of surveillance, intelligence, and control.

Communication scholar Oscar H. Gandy, Jr. (1993) identifies the underlying concept of "panopticism" as a technology of power realized through the practice of disciplinary classification and surveillance that he refers to as the "panoptic sort." The panoptic sort is a system of power that is guided by a generalized concern with rationalization of social, economic and political systems. It is considered a difference machine that sorts individuals into categories and classes on the basis of routine measurements. Gandy (1993) asserts that it is a discriminatory technology that allocates options and opportunities on the basis of those measures and the administrative models that they embody and inform. He also asserts that it is a system of power that is institutionalized by corporations and governments in the form of ubiquitous information systems.

Sophisticated, ubiquitous technologies and techniques such as computerized record keeping contain the inherit potential to create immensely wide-ranging and insidious panoptic techniques, thereby increasing the ability of institutions to control people without directing them, using the subtle pressures of internalized discipline. Foucault's conception of the panoptic machine therefore acknowledged the control

potential of computers and electronic networks, in which both the distribution of intelligence and the integration of surveillance mechanisms could be concurrently co-coordinated and controlled.

Kevin Robins and Frank Webster (1988) maintain that information technology and computer networking are indeed utilized by government and enterprise to exercise surveillance and control over action and information, rather than extend democratic freedoms in modern Western societies. As Robins and Webster (1998: 61) state:

> Technologies, as they have actually existed, have been constituted to watch and control, to control through watching. Information technologies – actually existing information technologies – extend this capacity. In them is perfected the ability to mobilize and control through watching and monitoring: power expresses itself as surveillance and panopticism, on the scale of the social totality…
>
> The cabled electronic grid is a transparent structure in which activities take place at the periphery – remote working, electronic banking, the consumption of entertainment or information, tele-shopping, communication – are visible to the electronic "eye" of the central computer systems that manage the network(s). The technical process of administrating the numerous electronic transactions is simultaneously and integrally, a process of observation, recording, remembering and surveillance. The electronic worker, consumer, or communicator is constantly scanned and his or her needs/preferences/activities are delivered up as information to the agencies and institutions at the heart of the network. Decentralized, sequestered, privatized activities and lifestyles are monitored from the diverse centers of power administration.

Giddens (1985) defines surveillance as a technology that takes the form of accumulated coded information utilized to administer the activities of persons and to direct supervision of activities by persons in authority. He suggests that direct supervision by organizations commands segments of a person's life, specific to that portion spent at work in an office or factory.

While information technologies allow for the decentralization of lifestyles, work and the industrial structure through various *locales*, thereby creating a certain level of autonomy, they concurrently permit increasingly centralized state and corporate co-ordination and observation. This demonstrates that there is a duality concerning the nature of control. In the context of information technology, control can be interpreted as multi-faceted and conflicted, especially if there are competing interests utilizing the same infrastructure. Competing interests are apt to use their own specific technological designs to further their interests.

2.4 Technological Control Through Design

Communication theorist Robin Mansell (1996) uses the notion of a "design principle" to illuminate how social actors and market players express their objectives through technological design. Her design principle acknowledges that an empirical analysis of both technical and social considerations is necessary, not just to understand the impact of technology upon the efficiency of enterprises, but also to determine how institutions and social actors articulate their respective agendas through technological design. As a result, Mansell (1996) distinguishes design as a model or system, from design as an intention or purpose. Design encompasses not a single intention but a diversity of intentions unfolding in time and space. Mansell (1996: 23) therefore observes the fundamentally social nature of design as a phenomenon grounded in human intentions. Accordingly, the word design "invokes the idea of intentionality or purpose on the part of social actors" (Mansell, 1996: 23). She notes that design is guided

sometimes by "individual self-conscious intent" and sometimes by "the intentions of collective actors that can only be assumed to exist." (Mansell, 1996: 23). These collective intentions are not uniform, but are a reflection of diverse and potentially competing and even conflicting interests. Design therefore is a mechanism that works to interpolate human intentions into technologies such as electronic networks. Intentions are determined by a "capabilities principle", which Mulgan (1996: 24) argues:

> draws attention to the centrality of human capabilities in the development and use of technical systems and the fact that such capabilities cannot be taken for granted in an inquiry into the social and economic implications of information and communication technologies.

Mainstream economic theory mostly assumes that all economic actors have the necessary capabilities to participate in the information society. The capabilities principle can be used to recognize that human beings are knowledgeable agents. Those capabilities arise from diverse experiences and they are the result of substantial investments of time and other resources.

In order to research and explain developments in the area of access to and usage of information and communication technologies, Mulgan (1996) recognizes that the user capability must be considered. In a more strict sense, this refers to the acquisition, development and accumulation of skills by people in order to appropriate technologies. According to Mansell (1996: 28), using this principle allows us "to uncover the deeper processes that shape the trajectories of advanced information and communication technologies."

To fully explore the impact of design, Mansell (1996) also suggests that scholarly research needs to examine engineering practices in-depth to determine what intentions

are being incorporated. Legal scholar Lawrence Lessig (1999) develops this idea further by arguing that a confluence of values can be embedded into technology through design. Lessig recognizes the fact that architecture, or code, can be used to regulate and control all aspects of electronic networks, or cyberspace. His book *Code and Other Laws of Cyberspace* identifies the fact that technological developments are not inevitable. Instead, technology as Lessig conceives of it is malleable. Subject to a multiplicity of social and economic factors that exert control over its development and deployment, Lessig does not conceive of technology as a transcendent force with its own volition. He argues that the development and deployment of technology is an entirely human contrived process. Accordingly, societal and organizational forces continually influence technological architectures. Lessig thus argues that the intrinsic structure of electronic networks do not guarantee the advancement of specific values.

Lessig's approach differs from those held by Marxist scholars and the Frankfurt School since he maintains that communication technologies can incorporate a multitude of values. While Marxists maintain that communication technologies are mainly tools of ideology and domination, and the Frankfurt School stated that technology is the automatic implementation of instrumental reason, Lessig believes that technology does not promise the advance of specific, predetermined values. Values that embrace any political or philosophical view can be implanted into technology by commerce, government or civil society, which can alter its character either positively or negatively.

Cyberspace is thus a realm that can be regulated, or coded, to either include or exclude libertarian or authoritarian tendencies. Networks can either be harnessed to

accommodate corporate or governmental control under the technocracy thesis, or can allow greater independence for civil society. Since network technology is built and not found in nature, values can be selected and embedded into technology at will. Effectively, this destroys the conception of networks as solely inflexible regimes of control, since network structure is determined by a deliberate series of choices that directly influence usages and impact.

Lessig (1999) notes that these values, embedded into technology, are achieved through the hardware and software that sets the protocol of network design. He argues that the entire architecture of cyberspace is achieved through code, determined by the architects or coders who design computer-mediated communication infrastructure. These architects can choose amongst designs. These choices are many and complex and effectively determine the architecture and culture of cyberspace. This occurs because both the space and experience that cyberspace provides is imposed through code. Because code is flexible and subject to change, it can define freedoms or impose constraints upon behaviour. This tears asunder both conceptions of cyberspace as only either an anarchical environment that cannot be regulated or as an environment of inexorable control.

Lessig (1999) argues that the nature of cyberspace cannot make it immune from the control of commerce or government because in essence cyberspace has no nature. It only has code: the software and hardware that make it what it is. Lessig therefore maintains that code creates a place of freedom and innovation, as he maintains the original architecture of the Internet did, or constructs a place of exquisitely oppressive

control. The freedom that cyberspace permits and the control that cyberspace allows are thus dependent upon code.

In real space, humans recognize mechanisms, such as constitutions, statutes and other legal codes, through which the law regulates. In relation to cyberspace, Lessig theorizes that we must also understand how code regulates, or how software and hardware that makes cyberspace what it is, regulates cyberspace as it is. Lessig therefore believes that code represents a new form of regulation.

Accordingly Lessig (1999: 6) proclaims that: "Code is law." Code works to reflect social interests that impact how we live and communicate. As technology becomes more important to different aspects of our lives, its legislative authority increases. The problem surrounding code however concerns who exercises the authority to promulgate it.

Feenberg (1992) recognizes that technological principles are insufficient by themselves to determine design. He believes technical choices are "underdetermined", and that the final decision between alternative technical designs ultimately depends on the fit between them and the interests and beliefs of the various social groups that influence the design process (Feenberg, 1992).

According to Feenberg (1995: 4), "technological designs are negotiated achievements involving many partners, not rational inspirations that spring full blown from the mind of an individual genius or pure laboratory research. The design process is the place where the various social actors interested in a developing technology first gain a hearing."

These social groups include business owners, individual users, technicians, customers, political leaders and government bureaucrats. Feenberg argues that the variety of social groups guarantees that designs represent a myriad of interests. They wield their influence by "proffering or withholding resources, defining the purpose of the devices they require, fitting them into existing technical arrangements to their own benefit [and] imposing new directions on existing technical means" (Feenberg, 1995: 4).

Technologies, he maintains are like other rational institutions: they act as social expressions of these actors. As a consequence, Feenberg (1995) also develops a notion of "technical code" to describe those features of technologies that reflect the hegemonic values and beliefs that prevail in the design process. Technical code is used to advance the control capacity of social groups vis-à-vis technology.

Feenberg however does acknowledge that control has a dual nature. Though he maintains that the control capacity over technology is mainly used to maintain managerial power, he does note technology's democratic potential.

Feenberg (1995: 6) observes that: "undemocratic design procedures have substantive consequences through the attempts by powerful players to preserve their technical initiatives and control in the communication systems they create. Their interest in maintaining that power is a kind of bottom line inscribed in all their technical decisions, biasing those decisions in the direction of centralization and hierarchy."

Feenberg (1995: 9) notes however that as: "more and more of social life is framed by technical systems, cases increasingly appear in which public interventions into technology determine the conditions of agency." Public action therefore leads to

appropriation of technology by groups that oppose undemocratic technical design deployed by powerful players such as governments and corporations. While the reigning common sense of many theorists discourage exploration of the democratic potentials of a technological society, Feenberg maintains that technology does retain a democratic potential. Technology therefore facilitates a duality of control characterized by imposition and confrontation. This duality is apparent upon electronic networks.

2.5 The Duality of Control Upon Electronic Networks

Control upon electronic networks alternate between competing interests. In all communication systems including electronic networks, Geoff Mulgan (1991) theorizes that: "[c]ontrol has a double nature ... One is the notion of control as exogenous, imposed, abstracted, and rationalized. The second is the notion of control as endogenous, as communicative and shared. ... The tension between the two ideas of control forms a dramatic fault line at the heart of all information technologies which simultaneously offer massive enhancements of both types of control" (Mulgan, 1991: 4).

For Mulgan, networks and other communication systems mainly serve as channels for societal control and are identifiable by way of the dual nature of their control capacity. Within his analysis, control is complex, multi-faceted and can be characterized as dialectic. Exogenous control is the capacity to exert influence over the environment, over systems and individuals outside a medium. Endogenous control, in contrast, is conceptualized as an internal system for regulating a system itself. The traditional concern with control, in this sense, is only preoccupied with top-down exogenous control.

Mulgan, however, points out that control can be exerted from the bottom up, or across the system (Bates, 1997).

Mulgan (1991: 4) notes that "[n]ew technologies have served to highlight the extent to which control is never simple or one-dimensional." To him, control is not an inescapable regime, as proposed by Beniger (1986) or the Frankfurt School (Adorno and Horkheimer, 1972). Control has multiple dimensions. As a consequence, the same information, communication and networking technologies that are essential to control, also brings with it new threats to those control mechanisms. Under Mulgan's conceptualization, control over information and communication technologies is actively contested. The social relations of power behind computer-mediated communication is normally associated with: limitations in access; communication competence; commercial interests; the public interest; public opinion; and government action or inaction. Though these specific limitations all pose constraints on the communicative capacities of electronic networks, Mulgan (1991) proposes that communication technologies concurrently contain features that permit for agency and action amongst people. Since critical theorists such as neo-Marxists and the Frankfurt School defined communication as asymmetrical information systems or limited communication relationships, information itself was perceived as strictly a controlled commodity, supplied from positions of authority to users that were positioned as either the consumer, or, as in the case of entertainment and leisure services, the audience.

Mulgan's approach to control, in contrast, acknowledges that the potential exists for true, unrestricted two-way communication and information systems that could be

influenced by the audience or general public. Channels of communication can therefore be influenced and directed not only by societal or corporate elites, but also by individuals and social groups with counter-hegemonic vantage points.

For Mulgan (1991), technology and the information revolution in particular, is best understood as an increase in capacities to control, which is exploited both by new horizontal social networks and by traditional hierarchies. In terms of social networks, the promise of the information revolution is that power can be distributed evenly. The fact that social activists and movements can leverage information and communication technologies give credence to a theory of contested control over technological resources. Electronic networks can ideally displace hierarchies, thereby empowering citizens against states and consumers and smaller vendors against large companies. Traditional hierarchies however can concurrently use networks to concentrate and reinforce their economic and social power.

Analysis by Mulgan (1991) therefore reveals that access to and control over electronic networks continually fluctuates between open and closed models. His interpretation of control is not constrained by the notion of an inescapable controlled or "engineered" society as advanced by G.T. Marx (2002). Instead, control is a phenomenon that develops to empower both communities and markets at different times. Control is therefore not simply a burden, a phenomenon that weighs down on people from above, or a pejorative concept. Instead Mulgan (1991: 8) argues that: "Control can be liberating as well as oppressive. Even as societies become more systematic and controlled, freedom and control pass to individuals and groups to be used in non-rational, anti-systemic ways.

Control is neither inherently good nor evil but rather a basic resource of advanced societies that needs to be understood both as to its potential and as to its limits. Like power and reason, it demands neither an excessive love nor an excessive fear."

Control, in effect, is characterized by its oscillation between dominance and resistance. Sociologist Anthony Giddens entitles this concept the "dialectic of control" in which subordinate groups are able (through making use of technological resources open to them) to exercise some control over super-ordinate groups, even if the balance is highly asymmetrical (Giddens, 1984: 283).

This duality in control is apparent in electronic networks where control also oscillates between different economic and social interests. Communication theorist Robin Mansell (1993) would recognize a duality of control while outlining emerging models of telecommunication network development during the late 1980s and 1990s in her book *The New Telecommunications: A Political Economy of Network Evolution.*

She argues that electronic networks can either adopt open or closed models of control. These two approaches assume an "idealist" form that is characterized as open, ubiquitous, transparent and demand-led; and a "strategic" form that is closed, fragmented, oblique and supply-led.

According to the idealist view, there is no need to implement regulatory measures in order to obtain ubiquitous and open networks since the market reallocates resources through fair and free competition. Since competition under such a scenario is open, so too is network design. Such network architecture allows for a high degree of innovation

and for ubiquitous service diffusion. Diffusion, by extension, automatically permits unencumbered multi-purpose use of networks by communities.

The idealist model of telecommunication development preferably provides for "the integration of information and communication services within a permeable seamless network" (Cited in Mansell, 1993: 7). As a result, boundaries between public and private networks disappear and the convergence of competencies across telecommunication and computing networks abolish the distinctive core competencies that divided these technologies in the past. Innovations permitted under the model allow for new entrants in equipment, network operator and service supplier markets, thereby eroding the market power of incumbents.

Under the idealist view, networks are regarded as a technological feat that provide both advanced services and fair, enhanced competition. Networks are envisioned as solutions that contribute to the competitiveness of the economy and to the political, social and cultural cohesion of markets and communities. The requirement for policy intervention and regulation was thought to have quickly dissipated as it could be replaced with market mechanisms that allow for a greater number of network operators and hence service options. Due to a belief in the creation of a larger pool number of network operators, the dominant belief was that the idealist network model was best suited to respond directly to the demands of a wide range of consumers.

According to Mansell (1993: 8): "The Idealist model assumes that the combined forces of technical innovation and competition will erode monopolistic control of the telecommunication infrastructure and the services it supports. In this model, PTOs

[public telecommunication operators] argue that the diffusion of an advanced telecommunication infrastructure and the entry of new service providers means that no single supplier can dominate the market sufficiently to foreclose entry or to discriminate unjustifiably among customers."

The opposite view, as represented by the strategic perspective, claims that full competition is not regarded as a likely outcome of network deployment. As a consequence, a few actors that avoid non-profitable customers dominate markets. Mansell (1993: 6) notes that under "the Strategic model there is continuous rivalry among a relatively small number of dominant firms" and that "rivalry, monopolization and institutional restructuring do not serve all market participants equally well." In the context of electronic networks, she argues the technical and institutional designs of networks that underpin market conditions represent a shift "not from monopoly to competition, but from monopoly to strategic oligopoly" (cited in Mansell, 1993: 21).

As a result, Mansell (1993) asserts that though the idealist model was rhetorically adopted and mystified by the telecommunication and network providers, in reality, network evolution primarily embodied characteristics of the strategic model. Within that model, the design of the network is supply-led, rather than driven by competition. This is important because, as the strategic view emphasizes, network design will continue to gravitate toward mechanisms that help to maintain or re-establish monopolistic power in the marketplace. Network segmentation, as implemented under the strategic model, results in greater flexibility and choice for multinational corporations that increasingly require advanced applications that support global finance and production. The

consequence of such a design is that it produces disadvantages for many other consumers in terms of network access and costs, and creates more complex network access conditions. Its also causes the development of new modalities of exogenous control, that inhibit the role of competition in the development of network infrastructure.

Mansell (1993) thus interprets the strategic model to be the dominant approach toward network development. She however does note that a competing, open vision of network control exists, and that a duality of control is a central feature of network evolution and design. As a consequence, control upon networks is not simply imposed, but contested by a myriad of social players.

Chapter 3 The Duality of Control in Network Design

A "duality of control" permeates network evolution and design. It is a recurring theme that greatly impacts how we understand the development of electronic networks. As computer networks have grown and dispersed throughout society, dialectical or competing visions of networks have emerged. This chapter juxtaposes these competing visions to illustrate how the struggle for control is played out in network environments. It demonstrates that the function and organization of networks, such as the Internet, can encapsulate either "open" or "closed" philosophies towards network design and development. These philosophies are embedded into the technological design of the network through code and are continually evolving. While electronic networks such as the Internet first emerged as an open resource that allowed wide user interconnection and little restriction on usage, it continually underwent a transition that effectively placed limitations on both usage and access. As business interests continually increase their investment in network and information technology in order to increase profitability and performance, their inclination is to exercise greater control over the technology. Enterprises achieve this through the introduction of closed network architectures. This chapter provides a thorough description of the open and enclosed network approaches in terms of technological engineering and evolution. In cursory terms, it also outlines the fluctuating contest for access to open network architecture by competitive firms and social groups, known as debates over network neutrality.

3.1 Open Architecture Networking

When the Internet first emerged in the popular imagination during the early 1990s, it was conceived as a disruptive economic and political force that could not be regulated. Its original design essentially established a digital networking model that was designed to be "open", permitting free and unfettered access to network resources and the ability to innovate at will. Open networks were the materialization of a communication philosophy that emphasized accessibility.

According to Lessig (1999), "openness" was the key determinant in the construction of the information society and its concomitant, original network architecture. Once users have access to open network architecture, they are free to attach any myriad of devices, information and applications to the communication infrastructure without restriction. The Internet, a prime example of an open network, was specifically designed to encourage the wide interconnection of affiliated networks and users. According to Vinton Cerf (2003), a co-designer of internetworking protocols, the Internet embodied one main technical idea: namely that of "open architecture networking". Under this approach, "the choice of any individual network technology was not dictated by particular network architecture but rather could be selected freely by a provider and made to inter-work with other networks through a meta-level internetworking architecture" (cited in Cerf, 2003). The resulting network design encouraged innovation, openness, sharing of computing and communication resources, and broad access and use.

The open end-to-end approach to networking was revered by the Internet's original engineers because it, in contrast to top-down control, encouraged control from

the bottom-up or by the end-user. In a now-classic paper on network engineering, Jerome Saltzer, David Reed and David Clark (1984) elaborated on the design approach for computer systems called the "end-to-end" principle. End-to-end arguments are those that take the position that: "[I]f a particular function requires the participation of the endpoints of the system, it should not be implemented in any more basic component or other location in the system" (Cited in Sandvig, 2006).

End-to-end arguments thus guided the placement of functions in a communication network. The objective behind "end-to-end" network logic was to implement open communication protocols that allowed networked computers and devices to communicate transparently across multiple, linked packet networks. Through employing this architectural design, the placement of functions within a network was open and highly structured, providing power to users at the end of the network (Lessig, 2002).

The "end-to-end" architecture specified that application-level functions usually cannot, and preferably should not, be built into the lower levels of the system, or the core of the network. Instead under the "end-to-end" model, intelligence in the network was located at the top of a layered system, or at its "ends", where users themselves could place knowledge and information processing capacity (Lessig, 2002).

Typically, network designers distinguish computing resources at the "end" or "edge" of a network from computing resources within that network. The resources at the end of the network are the devices utilized to access the network, such as personal computers or cellular phones with digital services. The computing resources within the

network are devices that establish links to other computers, thereby forming the network itself. Such resources include physical servers and firewalls (Lessig, 2002).

According to "end-to-end" arguments, such as those identified by that National Research Council (2000: 30) in the United States, computing resources within the network should only perform very simple and standard functions that are required by the majority of network applications, while functions that are needed by specific applications should only be performed at the network's edge:

> Aimed at simplicity and flexibility, [the end-to-end] argument says that the network should provide a very basic level of service – data transport – and that the intelligence – the information processing needed to provide applications – should be located in or close to the devices attached to the edge [or ends] of the network.

One consequence of this design is the principle of non-discrimination among applications. Lower-level network layers in the "end-to-end" system provide a broad range of resources that are not particular to or optimized for any single application – even if a more efficient design for at least some applications is thereby sacrificed (Lessig, 2002). As described in a subsequent paper by Reed, Saltzer and Clark (1998: 69):

> End to end arguments have ... two complimentary goals: (1) Higher-level layers, more specific to an application, are free to (and thus expected to) organize lower level network resources to achieve application-specific design goals efficiently (application autonomy); [and] (2) lower-level layers, which support many independent applications, provide only resources of broad utility across applications, while providing to applications useable means for effective sharing of resources and resolution of resource conflicts (network transparency).

When the Internet first emerged, according to Lessig (2002), its network designers located intelligence at its "ends" where users put information and applications

onto the Internet. Through placement of user applications at the edge rather than the core, the network encouraged a high degree of flexibility for users.

Lemley and Lessig (2000) maintain that this capacity to deploy applications to the network with little restriction ultimately led to an unprecedented amount of economic, cultural and scientific innovation. They argue that end-to-end principles expanded the competitive development of Internet services by enabling a wide array of applications to connect and utilize the network. As there is no single strategic actor under an "end-to-end" network regime who can influence the competitive environment (the network) in favour of itself, nor any hierarchical entity that can favour certain applications over others, an end-to-end network created an extremely competitive environment and a robust culture for innovation. Since end-to-end design is not optimized for any particular existing application, the network is open to innovation that had not been originally imagined (Lessig, 2002).

As Saltzer, Reed and Clark (1998: 70) argued "had the original Internet design been optimized for telephony-style virtual circuits ... it would not have enabled the experimentation that led to protocols that could support the World Wide Web, or the flexible interconnect that has led to the flowering of a million independent Internet service providers. Preserving low-cost options to innovate outside the network, while keeping the core network services and functions simple and cheap, has been shown to have very substantial value."

By keeping the network simple, and its interaction general, end-to-end proponents such as Lessig (2002) have argued that the Internet facilitated new applications that could

not have originally been envisioned. To take just a few examples, Internet telephony, digital music transfer, and electronic commerce are all applications far outside the range of expectations of those who designed the Internet. During its embryonic stage in the mid-to-late 1990s, firms obtained unimpeded access to the Internet, allowing them to deploy hardware or software solutions that they developed, in order to create and offer new services (Lessig, 2002). Lessig (2002a: 1788) defined this initial environment as a commons: "a resource which is free" but which is "not necessarily zero cost."

A commons permits anyone to access and to use a resource without requiring the explicit permission of anyone else. Lessig (2002a: 1789) maintained that the commons was a central feature to the Internet's initial design, especially its higher layers that permitted unfettered control by all over basic network functionality:

> [I]nnovation on the Internet didn't depend upon the network. New content or new applications could run regardless of whether the network knew about them. New content or new applications would run because the network simply took packets of data and moved them along. The fundamental feature of this network design was neutrality among packets. The network was simple, or "stupid" in David Isenberg's sense, and the consequence of stupidity, at least among computers, is the inability to discriminate. Innovators thus knew that, if their ideas were wanted, the network would run them; that this network was architected never to allow anyone to decide what would be allowed.
>
> This means that this layer of this network - this feature of the network that distinguished it from all that had been built before - built this network into a commons. One was free to get access to this network and share its resources. The protocols were designed for sharing, not exclusive use. Discrimination, which lies at the heart of a property system was not possible [with end-to-end]. This system was coded to be free. That was it nature.

By utilizing standardized network routing techniques aided by ubiquitously available technical standards and protocols, any user, device or application could interconnect to the network and interface with each other. End-to-end advocates such as

telecommunication engineer David Isenberg (1997) in fact argued that the network should be "stupid", or devoid of any intelligent capacity that effectively controls network traffic. His vision of a new network philosophy and architecture entailed the development of a fully accessible, public communications network. Under this model, electronic networks would be engineered for intelligence at end-user devices, not in the network.

Brian E. Carpenter, a director of Internet standards and technology at IBM, also concurred with this assessment. As a member of the Internet Architecture Board, a committee of the Internet Engineering Task Force, his observations were that "in very general terms, the [engineering] community believes that the goal [of electronic networks] is connectivity, the tool is the Internet protocol, and the intelligence is end-to-end rather than hidden in the network" (Cited in Carpenter, 1996).

The predominant belief amongst engineers is that the exponential growth of electronic networks illustrate that connectivity is its own reward, and is often more valuable that any individual application such as electronic mail or the World Wide Web. Additionally, Carpenter (1996) maintained that standardized protocols were also a defining hallmark of global electronic networks:

> It is generally felt that in an ideal situation there should be one, and only one, protocol at the Internet level. This allows for uniform and relatively seamless operations in a competitive, multi-vendor, multi-provider public network.

Carpenter recognized that connectivity required a level of technical co-operation between service providers. Connectivity can flourish on a global scale if an "open" inter-network approach is taken towards protocols in particular, and architecture in general.

Under an open regime, networking protocols were to be independent of the hardware medium and hardware addressing. This approach allowed open networks such as the Internet to exploit any new digital transmission technology of any kind, and to decouple its addressing mechanisms from the hardware. It allowed open networks such as the Internet to be an easy method to interconnect fundamentally different transmission media, and to offer a single platform for a wide vary of information infrastructure applications and services.

Robert Kahn (cited in Cerf *et al.*, 2003), another one of the original designers of the Internet, had also initially conceptualized interconnected electronic networks as essentially open environments:

> The Internet was based on the idea that there would be multiple independent networks of rather arbitrary design ... The Internet as we now know it embodies a key underlying technical idea, namely that of open architecture networking. In this approach, the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to inter-work with the other networks through a meta-level "internetworking architecture."

In open network architecture, individual networks were separately designed and developed, and each had its own unique interface that it could offer to users and to other providers, including other Internet and telecommunication firms. The main characteristics of open network architecture according to Kahn (cited in Cerf *et al.*, 2003) were:

(i) Each distinct network would have to stand on its own and no internal changes could be required to any such network to connect it to the Internet;

(ii) Communications would be on a best-effort basis. If a packet of data did not make it to the final destination, it would shortly be retransmitted from the source;

(iii) "Black boxes" would be used to connect the networks; entitled gateways and routers. There would be no information retained by the gateways about individual flows of data packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery from various failure modes; and

(iv) There would be no global control at the operations level.

According to Kahn, there are generally no constraints on the types of networks that can be included in open network architecture or their geographic scope. As a consequence, open networks deliver data packets without discrimination. This characteristic allowed networks to become ubiquitous within advanced economies.

Indeed, the Internet flourished due to the interconnectedness of nodes upon the network. With few restrictions placed upon the interconnection of gateways, routers and other devices, the Internet experienced exponential growth. Routers and gateways, the fundamental components that facilitate network traffic and control, allowed ever-increasing amounts of data to traverse the network because they did function as "black boxes".

Lawrence G. Roberts (2002), one of the Internet's first architects, optimistically estimates that U.S. Internet traffic had a 280 percent annual compound growth rate through the year 2000 and had increased 300 percent per year over the next five years. Mathematics professor Andrew Odlyzko (2003) more reasonably estimates that backbone traffic had approximately doubled each year, translating into a growth rate of between 70 and 150 percent, as indicated in the following table.

year	TB/month
1990	1.0
1991	2.0
1992	4.4
1993	8.3
1994	16.3
1995	?
1996	1,500
1997	2,500 - 4,000
1998	5,000 - 8,000
1999	10,000 - 16,000
2000	20,000 - 35,000
2001	40,000 - 70,000
2002	80,000 - 140,000

Table 3.1.1 – Annual U.S. Internet Backbone Traffic; Estimated traffic in terabytes during December of each year. (Odlyzko, 2003: 2)

According to the Internet Domain Survey (2003), conducted by the Internet Systems Consortium, network domain registrations (the names assigned Internet servers and nodes) grew from 1.3 million in 1993 to 171.6 million in January 2003. The Online Computer Library Center (2003) estimates that the number of distinct Web sites on the Internet (the popular network mechanism used to transmit content) grew from 2.8 million in 1998 to 9 million in 2002. The number of total visible hosts, or computers and other devices upon the Internet increased from four million in 1995 to over 350 million by 2004, according to both the Internet Systems Consortium (2005) and the Center for Next Generation Internet.

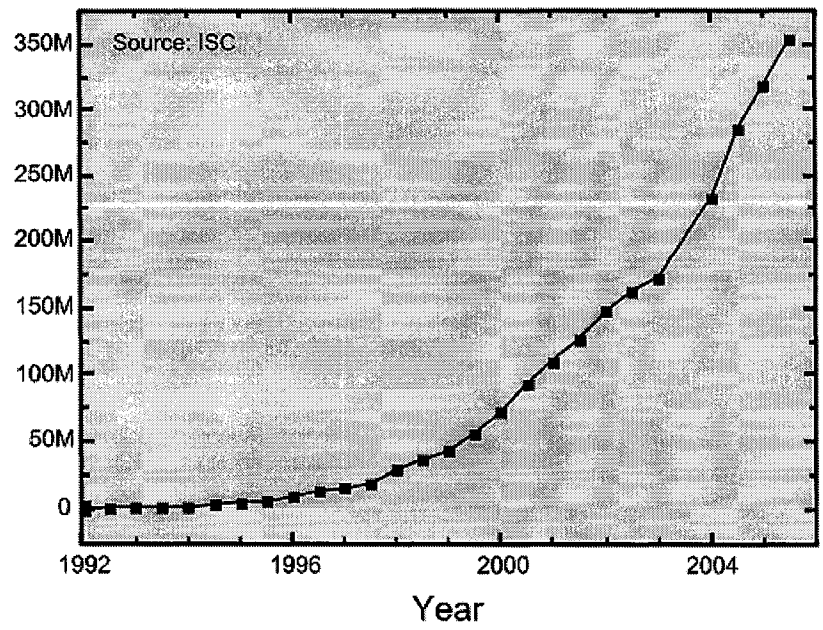

Chart 3.1.1 – Number of Visible Internet Hosts: 1992-2005 (Internet Systems Consortium, 2005)

In terms of usage, the Internet grew from a small cadre of expert institutional users to a large number of users. A survey of multiple Internet users estimates shows that the number of network participants worldwide has concurrently risen with the number of nodes deployed. Estimated worldwide Internet usage has grown from 16 million users in 1995 (IDC, 2005) to approximately 700 million users in 2005 (ComScore Networks, 2006), underscoring the fundamental consequence of open network architecture for access.

Tremendous user growth was possible due to the open, end-to-end design of the Internet, which encouraged network intensification and expansion. Lessig (2002: 36-37) claims that this network design had fundamental consequences for innovation: "Firstly, since applications ran on computers at the edge of the network, innovators with new

applications needed only to connect their computer to the network to allow their applications to execute. Consequently, no modifications to the computers, or nodes within the network were required. Secondly, because the network design was not optimized for any particular existing application, open networks could accommodate new application designs without technical constraints imposed by the network. Thirdly, since the design created a neutral platform (neutral in terms that the network could not discriminate against specific data while favoring other data), the network did not discriminate against new applications."

The significance of these consequences was that a large degree of control over network resources was entrusted to end-users. Consumers and end-users at the edge of the network not only had basic access to the network, but the ability to contribute to its basic structure by actively deploying resources that could influence how traffic is routed, and how information is manipulated.

Most importantly, under the end-to-end network model, users at the edge were able to exert substantial influence over the technical development of standards and protocols and openly experiment with variations without experiencing technical constraints imposed by the network. The end-to-end network model engenders an approach to network design that encourages the active participation of a wider array of users and uses. For business, open networks allow smaller firms to quickly develop and deploy competitive new information products and services without technical restrictions from incumbent service providers. The architecture therefore facilitates the creation of services that rivaled those offered by major telecom and network operators.

Independent providers could offer narrowband Internet access over dial-up telephone lines. This generation of Internet provision allowed any user to connect any custom application or device to the network architecture. Such services were made possible through regulatory regimes in North America that required incumbent telephone companies to treat both their customers and competitors in a non-discriminatory manner and allow for network interconnection.

According to consumer advocate Mark Cooper (2003: 179) these factors allowed networks to remain accessible to consumer and citizens, who leveraged open communication platforms to promote "a dynamic space for economic innovation and a robust forum for democratic discourse." For Cooper (2003: 179), "[t]he role of regulation [was] to ensure that strategically placed actors [could not] deter expression or innovation at any layer of the communication platform. This [was] best achieved by mandating that the core infrastructure of the communication platform remained open and accessible to all."

3.2 Transition Towards Network Enclosure

Technological change ensured that regulated network designs would evolve so that network operators could self-regulate the core infrastructure of the communication platform. In his book *The Future of Ideas: The Fate of the Commons in a Connected World*, Lessig (2002) indicates that the nature of networks changed so that regular users and small businesses increasingly could not exercise control over basic network functionality. New mechanisms of control and regulation had emerged that were

transforming electronic networks from "open" to "closed" environments to explicitly benefit large corporations.

Previous mechanisms of control had been endogenous, allowing all participants on the network to deploy applications and execute alterations and improvements throughout the architecture at anytime. In contrast, the new mechanisms of control that were emerging were exogenous, or imposed, and highly structured, allowing for no alterations unless specifically and explicitly permitted.

While Lessig (2002) initially conceived of the ideal network architecture as simple and without intelligence interpolated into network design, emerging new architectures are more complex, incorporating intelligence into the network through technological intermediaries.

An intermediary is a computational element that lies between an information producer and an information consumer (Barrett and Magilo, 1999). The emergence of technological intermediaries allows third parties, such as network operators and telecommunication firms, to exercise a higher degree of control over ubiquitous and global computer networks. Unlike "open" end-to-end designs, the "end-to-intermediary" approaches offer network operators the capacity to co-ordinate and centralize network operations, functions and architecture. The use of such technologies allows third parties to set policies that establish clear boundaries for users.

Intermediaries, in effect, provide third parties with the tools to discriminate between users on the basis of identity, geography and service performance requirements. The technologies achieve this objective by embedding information and sophisticated

devices into the core of the network. By locating technological intermediaries into the "hubs" of the network architecture, enterprises and service providers can achieve greater levels of management over network resources by filtering and prioritizing selected data transmissions for specific applications. By employing this type of "end-to-intermediary" architectural design, intelligence comes to be situated closer to the centre of the network.

Utilizing intelligent network routing equipment and software, rather than unintelligent "black boxes", enterprises and network operators can identify user applications and classify network traffic on the basis of priority, thereby ensuring that specified transactions have higher-priority and are guaranteed delivery before other traffic. They can also limit application deployment, and control and limit the transmission of specific types of content, thereby restricting application development. End-to-end proponents such as Lessig (2002), therefore, have argued that imposition of "end-to-intermediary" architectures on the Internet will likely retard innovation by individuals and small enterprise due to its inherit discrimination amongst applications.

Large enterprise users of the Internet maintain however that discrimination is required to ensure greater application functionality and control in ubiquitous computing environments. Discrimination allows businesses to access new mechanisms of "structured extensibility" with confidence in order to control their global operations. Structured extensibility facilitates systems of economic mass collaboration in diverse computer-mediated environments in order to facilitate global coordination of corporate resources. Since corporations would increasingly depend on the Internet, as outlined in chapter one, they would seek i) enhanced quality of service and ii) tightened control over

their network resources. Service providers would respond to these requirements through the introduction of new intelligent network architectures, which incorporated the use of a new generation of advanced, high-speed Internet access technologies known as broadband.

With frameworks of structured extensibility broadening networks by integrating a wider range of technologies into a highly integrated system of economic relationships, corporations demanded network architectures that guaranteed reliability. Since end-to-end network architecture was predicated upon "best effort service," or basic raw network connectivity without guaranteed data delivery, corporate customers elected to implement end-to-intermediary architectures over open network systems such as the Internet. The new architectures would encapsulate intelligence and control functions into the centre of electronic networks. By so doing, the new intelligent network designs violate Kahn's original characterization of open architectural principles.

3.3 Closed Architecture Networking

Under the emerging end-to-intermediary, intelligent network model, intelligence is taken out of the ends of the networks or switches and placed in computer nodes that are distributed throughout the network (International Engineering Consortium, 2005). This approach provides the network operator with the means to develop and control services more efficiently. The result is the imposition of a network architecture that permits service providers to implement new technical constraints upon electronic networks in order to restrain competitive pressures, add surveillance capacity, deploy customized

applications for priority customers and develop new sources of revenue. Intelligent networks provide the capability to provision new services or modify existing services throughout the network instantly. Once introduced, services are easily customized to meet individual customers needs (International Engineering Consortium, 2005). The intelligent network aims to ease the introduction of advanced services based on more flexibility and new capabilities.

In an intelligent network, a substantially greater degree of information-processing capability resides within the network as compared to the traditional capabilities of the infrastructure. Intelligent networks provide telecom and other network operators with more flexible and cost effective methods of meeting customers requirements, especially by enhancing customer control and providing a greater degree of customization to the particular business needs of the organization. Overall, large enterprises require the extensive provisioning of cost-effective communications for voice, data and image applications across the entire business spectrum, from suppliers, manufacturers, distributors, wholesalers, retailers and customers, all of whom are increasingly globally distributed. The closed network architecture underlying intelligent networks offers corporate and business customers an effective option to manage all of the above requirements.

For telecommunication providers, the main benefit of intelligence networks is the ability to overlay new network services on existing public network infrastructure and develop new sources of revenue. The implementation of intelligent networks allow for the rapid introduction of new services by the telecommunication firms themselves for

global enterprises. The firms also gain the capability to provision new services and modify existing services throughout the network without physical intervention (Chen and Yang, 1999).

The implementation of intelligent networks further modifies the way that equipment vendors, customers and telephone companies operate their business and interrelate with each other. Under the intelligent network, or "end-to-intermediary" model, vendors define and develop standards-compliant products that shift design control and responsibility to the network operator or telecommunication provider. Network users only gain access to new services and custom solutions through the telecom or cablecast provider, who offers intelligent services vis-à-vis high-speed proprietary architectures (Bar *et al.*, 2000).

These new architectures, which include digital subscriber line (DSL) and cablecast systems, combine the transmission conduit with access. The architecture of the new "broadband" technologies is therefore different than end-to-end narrowband network services since they bundle Internet service along with the communication network itself. By bundling service provision with access, and by not permitting users to select another, independent service provider, the architecture removes the competition that existed under the narrowband model. By eradicating competition, the architecture removes an important barrier to any strategic behaviour that a telecommunication or cable company might engage in. The closed architecture, therefore, represents a significant change from end-to-end design since there is, in principle, no limit to what intelligent network

technology the telecom or cable provider can bundle into the network, due to its total control of the network (Bar *et al.*, 2000).

As network services evolve beyond the functions that they had traditionally performed, telecom and cable providers are placed in a position to foreclose all competition in an increasing range of services provided over broadband lines. The consequence of re-bundling network services under the closed model is that no effective competition amongst independent service providers would exist. The captive service provider operated by the telecommunication or cable network operator determines the range of services available to broadband users. They would determine through technological control ingrained within an intelligent architecture whether, for example, full length streaming video is permitted, whether customers can resell broadband services, and whether broadband customers can become providers of specific Web content or access other content. Under the captive service provider approach, network operators would have the power to determine what Internet services to allow. Customers who required network access, in turn, would have to accept that choice (Bar *et al.*, 2000).

Allowing the owner of the actual network to discriminate and determine network usage is fundamentally inconsistent with "end-to-end" design since only the broadband service provider would be able to influence the development and use of broadband technology. Furthermore, they would be exercising that influence not at the ends of the network, but at the centre. Consequently, a shift in control over innovation occurred, transferred from a variety of users and programmers to incumbent telecommunication and network operators.

3.4 The Principle of Network Neutrality

Lessig (2001) and Saltzer (1999) maintain that a shift to closed network design defeats the principle of networks acting as neutral environments that empower users. For the scholars, proprietary intelligent network designs are a first step towards a return to the old monopoly architecture over infrastructure and interconnection that existed before equipment deregulation. Within such an environment, the dominant operator had control over the architecture and exercised its incentive to design, deploy, maintain and control a closed architecture to better enable its own legacy business models.

Telecommunication history shows that network operators have traditionally gravitated towards closed systems. The most dramatic example of monopolistic control was that which AT&T exercised over its own telephone systems before the gradual introduction of competition in the United States. According to an early Federal Communication Commission regulation (FCC Tariff 132; 1947): "No equipment, apparatus, circuit or device not furnished by the telephone company shall be attached to or connected with the facilities furnished by the telephone company, whether physically, by induction or otherwise." The result was that AT&T as network operator had total legal control over all equipment that interconnected to its network from inception until 1968. Unencumbered legal control meant that only the incumbent telephone company could determine what products and services were offered over its infrastructure.

As Mulgan (1991) asserts, control is a contested terrain, and as such, it is not only imposed, but can also be opposed. The implementation of such heavy-handedness over network resources would be expected to breed opposition. Pressure was indeed

placed on the telephone company from third parties to develop new applications for the network. Since the telephone company was not responsive to such requests, innovations developed by independent equipment manufacturers had a hard time to succeed or find a market. The result was that the telecom had effective control over technological innovation.

In 1959, a private company in the U.S. challenged the telephone company's authority by developing a new device that permitted users of mobile radio systems to interconnect their landline telephone with the radio system to allow mobile and fixed users to communicate with each other. Though AT&T opposed the device, the private company filed a legal complaint based upon anti-trust measures, and managed to obtain approval from the FCC in 1968, opening the door to new innovations (Oxman, 1999).

Competitive manufacturers of equipment were able, by means of the Commission's new equipment registration and certification procedures, to build and deploy a wide variety of voice and data equipment for use with the public network, without seeking prior permission from monopoly telephone companies (Oxman, 1999). Through liberalized regulatory approval, the Commission allowed for the development and growth of manufacturers of devices that interconnected with the telephone network and offered value-added services and capabilities.

Deregulation facilitated the rapid deployment of devices such as the modem. Modems allow consumers with a computer and a telephone line to access data services, requiring no network alterations by the telephone company. Residential modem use, in turn, drove the majority of the growth of electronic network applications as consumer use

of networks increased. Indeed, without FCC regulations, users of public switched networks would have never been able to connect their computers and modems to the network, and it is likely that the Internet as it evolved in the 1990s would have been unable to develop (Oxman, 1999).

According to Bar *et al.* (2000), the use of the Internet in the United States had fundamentally rested upon 30 years of consistent FCC policy which sought to maintain network openness by making key network components available to all, on cost-effective terms, so as to foster competition and innovation. With the emergence of the new generation of Internet access technologies however, defined as "always on" broadband cable and telephony-based digital subscriber line, this openness was challenged by closed-access, proprietary technical controls that network operators could institute upon network infrastructure.

The fast growth of broadband adoption ensured that debates over architectural design and access became a mainstream political issue in the United States. According to a Pew Internet Project (2005) survey, approximately five million Americans had high-speed connections at home in June 2000. By May 2005, about 66 million Americans had high-speed connections at home. That number represented 53 percent of all Americans who go online from home, or 33 percent of all adult Americans, as represented on the following chart.

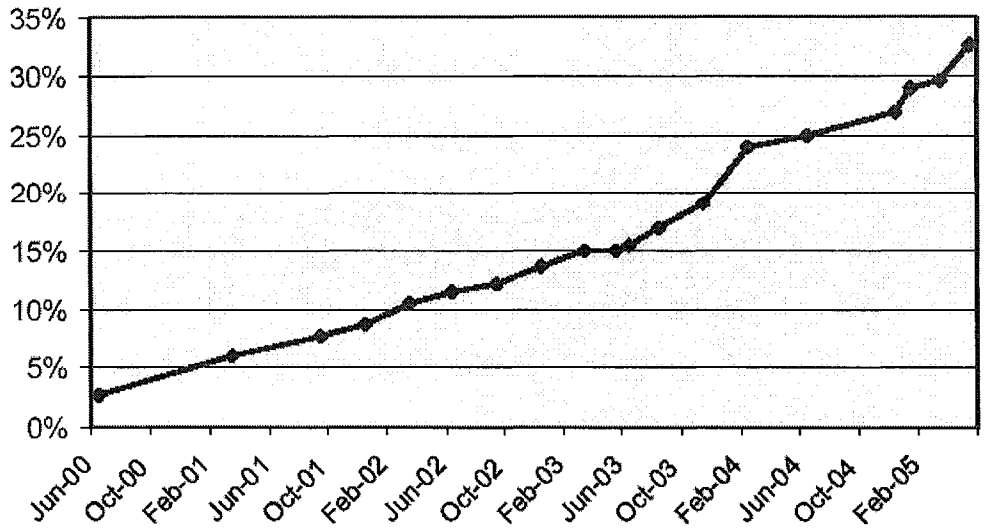

Chart 3.4.1 – Percentage of Adult Americans with Broadband at Home (Pew Internet Project, 2005: 6)

With such a rapid uptake of broadband Internet connections, concerns emerged about network neutrality. Network neutrality is a principle that ensures that all Internet users can access content or run the applications and devices of their choice, based on government regulation. With network neutrality, the network's only purpose is to move data, not to choose which data to privilege with higher quality service. The principle of network neutrality therefore prevents companies that own the infrastructure from discriminating against content based on its source or ownership. The principle of network neutrality argues that service providers cannot discriminate against rivals in terms of network access or traffic prioritization (Wu, 2003).

According to legal scholar Tim Wu (2005): "Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network

to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are less specialized - when they are a platform for multiple uses, present and future."

Network neutrality, in essence, applies common carrier style rules to Internet service providers, requiring that all Internet traffic be managed on equal terms, to ensure that all Internet content and applications remain equally accessible to all users. The notion of neutrality therefore draws heavily upon the legacy of the end-to-end, open architecture. Network neutrality supporters argue that a network should not favour one application, for example the World Wide Web, over another, such as online video. Drawing upon the end-to-end principle, they state that networks should incorporate a levelled balance between applications (Wu, 2003).

An end-to-end infrastructure routes all data with equal priority, ensuring that applications such as Voice over IP (VoIP), video, file sharing and electronic mail have equal treatment. With the advent of end-to-intermediary infrastructure however, communication firms who own the actual infrastructure that the data is routed through can prioritize bandwidth for their own financial gain and competitive advantage. The implication for such prioritization, or "traffic shaping", is that firms can tilt the playing field in favour of their own specific applications. A telephone company creating its own VoIP service, in direct competition with other Internet-based telephony services, for example, could selectively decide on speeding up their own service, while keeping the competitors at the same level. Such selective behaviour leads to the development of a "two-tiered" Internet, where separate classes of users and suppliers emerge.

Tiered Internet service is problematic for independent service providers since it limits the potential for their existing products and for potential innovation. With large communication firms able to exercise total control over network interconnection, speed and access, smaller competitors could be placed at a strategic disadvantage. Cost-of-entry to Internet marketplaces could become prohibitively expensive if large communication firms decide to dramatically increase the price of broadband access. Further, innovation could be stifled since there would be no guarantee that a broadband provider's selective behaviour toward certain preferred services could be moderated.

Communication firms argue that their selective behaviour would be justified because they build, own and operate their own broadband network connections and therefore should have the autonomy to charge differentiated fees for their usage. Applications such as VoIP and peer-to-peer networking and file sharing use a higher volume of bandwidth, causing other applications to slow down. Consequently, this forces network operators to bolster their physical infrastructure, which they argue costs a lot of money. Due to the increased expense, service providers believe they should get a greater return on their investment by charging independent content and service providers for increased network usage. Proponents of network neutrality however state if service providers are allowed to level more fees for preferential access, they will in fact be double billing for network access. End-users would first pay for access, and then end up paying additional broadband charges for services rendered by independent service providers.

Due to the perceived stakes in terms of access and cost, this conflict between discriminatory and non-discriminatory models of networking is currently playing itself out in the political arena. The proposals for implementing network neutrality have recently taken the form of various draft laws and regulations to govern Internet communications. These rules include commercial interconnection agreements between Internet Service Providers (ISPs), communication carriers, Internet content providers, and broadband users, usually on the basis of principles of public service obligations associated with special access to public rights of way. In this sense, network neutrality refers to a regulated condition in which Internet providers offer interconnection services on a uniform basis, without discrimination.

Typically, large Internet content providers (Google, *Yahoo!*, Microsoft, Amazon.com), consumers-rights groups (the Consumers Union), and trade associations (American Electronics Association) support network neutrality regulations. Opposition to network neutrality regulations generally comes from large communication carriers (Verizon, Comcast), manufacturers of network equipment (Cisco Systems, Nortel Networks, Qualcomm), and free-market advocacy organizations (Center for Individual Freedom, Cato Institute).

All of these groups are currently lobbying the U.S. government for legislative solutions in order to determine which model of networking will predominate. As of

November 2006, six proposed acts have been introduced in the U.S. Congress dealing with network neutrality but none have passed with any neutrality provisions intact.[1]

As a result, the development of Internet control technologies has outpaced the promulgation of legislation. While deliberations continue concerning the regulated deployment and use of control technologies, networking companies continue to develop them. The consequence is that technologies of network regulation have achieved wide proliferation amongst service providers in the form of technological intermediaries.

[1] The proposed acts include: *S. 2360, Internet Non-Discrimination Act of 2006*; *H.R. 5252, Network Neutrality Act of 2006*; *S. 2686, Communications, Consumer's Choice and Broadband Deployment Act of 2006*; *H.R. 5417, Internet Freedom and Nondiscrimination Act of 2006*; and *S. 2917, Internet Freedom Preservation Act of 2006*. *H.R. 5252, the Communications, Opportunity, Promotion and Enhancement Act of 2006* passed the U.S. House of Representatives, but network neutrality provisions were excluded.

Chapter 4 Technologies of Network Regulation

The use of technological intermediaries to regulate network environments is mainly characterized by the implementation of control technologies and the centralization of network resources. This chapter provides an overview of the different strategies and technologies that are used to assert monopolistic control over network resources, especially those on the Internet. It claims that changes in network access, approaches to interconnection and the implementation of new technologies all contribute towards enhanced control policies. These policies in effect act as mechanisms that enforce authority and the ability to manage or direct network resources. Electronic networks are environments that can be controlled *in toto*. Control however is not a mechanism that simply is imposed by enterprises and service providers in an effort to override openness. The depth of control is greater with concern to electronic networks since control is always a latent component of network architecture.

Control is not simply imported as an after-thought by enterprises to ensure corporate dominance. Control has always been an inherit component of networks, because in order for networks to function, networks needs to establish systematic management and organization. Open network design created the structural conditions necessary to exercise basic control over network infrastructure. Such a systematic approach is entitled *protocol*, which is a set of rules that define an exact format for communication between systems. Protocol, in terms of the Internet, is designed to ensure orderly communication between disparate computing systems and networks while at the same allowing for the widest possible interconnection (Galloway, 2004). The original

protocol devised for the Internet promoted open modalities of network control, in which unfettered power was granted to network users over access, applications and the deployment of devices at the network's edge. This chapter provides a technical overview of both open and closed modalities of control as represented by i) the original Internet protocol that promoted openness and ii) Quality of Service (QoS), structured extensibility, and centralized network resources, which promoted enclosure.

4.1 Internet Protocol: The Evolution of Open Modalities of Network Control

Computer engineers Vinton Cerf and Robert Kahn (1974) developed the Internet's original, open design protocol for packet network intercommunication in 1974. Entitled transmission control protocol (TCP), its main objective was to enclose packets of information into "data grams". These data grams were akin to envelopes containing letters. The content and format of the letter was not important for its delivery. The information on the envelope was standardized to facilitate delivery. Gateway computers would simply read only the delivery information contained in the data grams and deliver the contents to host computers. Only the host computers would actually "open" the envelope and read the actual contents of the packet. TCP allowed networks to be joined into a network of networks, or what we now call the Internet.

During the 1970s, Cerf continued to modify the protocol. He and colleagues decided to split the protocol into two. They took the part of TCP that was responsible for routing packages and formed a separate protocol called the Internet Protocol (IP). TCP would remain responsible for dividing messages into data grams, reassembling messages,

detecting errors, putting packets in the right order, and resending lost packets. The new combined protocol was called TCP/IP. In the TCP/IP suite, TCP was to provide guaranteed services while IP provided best effort delivery (Forouzan, 2003).

TCP performed the equivalent of obtaining a delivery confirmation from the recipient and returning it to the sender. Because IP provided basic packet delivery services without guarantees, it was identified as a "best effort" delivery service. It did its best to deliver packets to the destination, but took no further action to recover packets that were lost or misdirected (Forouzan, 2003).

The early Internet protocol suite consisted only of TCP and IP (although IP was not differentiated as a separate service). During development, TCP protocol designers identified a need for timeliness rather than accuracy. Speed, therefore, was more important than packet recovery, and though TCP was supposed to offer guaranteed services, this did not always occur (Forouzan, 2003).

Concerning real-time data, network designers of the "end-to-end" architecture, like Cerf and Kahn (1974), argued that a few lost packets were tolerable. Recovering them created excessive overhead that reduced performance.

Eventually, TCP was reorganized into TCP, IP, and user data gram protocol (UDP). The basic data addressing and data packet forwarding services in the network layer was called IP. TCP and UDP were in the transport layer on top of IP. Both used IP services, but UDP was a stripped-down version of TCP that provided applications with access to IP's best effort services (Forouzan, 2003). Applications went through UDP when they did not need TCP's services. UDP however was a "connectionless" protocol,

because, unlike TCP, it did not require the sender and receiver to establish a connection before data was transmitted. For this reason, UDP was considered unreliable because it did not guarantee that data grams would arrive in the same order they were sent, or even that they would arrive at all. The only improvement that the protocol did offer was slight error checking capacity, but this characteristic did not effectively enhance service levels. The protocol still only worked to reinforce a "best effort" network design that did not provide any guarantee of data delivery (Forouzan, 2003).

With best effort services, packet discard is deemed acceptable because recovery is handled by other services. In the lower physical and data link layers, data frames may be corrupted and dropped. In the network layer, congested routers drop data packets. It is the responsibility of the applications at the "ends" of the network to correct these issues. The first Internet protocols therefore did sacrifice performance, but in return allowed any users to exact a large measure of control over network resources by permitting applications at the network's edge, deployed by users themselves, to determine how data packets ultimately should be directed.

The next generation of network design, in contrast, sought to remove the best effort architecture in order to improve performance of business applications. With enterprises aiming to improve their productivity and profitability in a global business environment, they increasingly depended on the efficiency of networked applications. As a result, application performance became a critical consideration, as corporations identified the need to optimize network use in order to increase business value. Key components of network optimization were defined by user satisfaction, guarantee of

proper operations, cost reduction, risk management and control of complexity. Obtaining compliance to minimal levels of performance required business network optimization solutions that were designed to automatically manage and maximize network application performance based on demand. Such solutions could only be supported by end-to-intermediary architecture, implemented and controlled in its entirety by a service provider, since comprehensive control over service levels required the use of guaranteed services. Consequently, businesses needed network infrastructures that would guarantee full reliability. Such architecture is dependent on newer mechanisms that assure the performance of critical applications over the network while preserving the performance of all other applications and controlling telecom costs. These mechanisms included dynamic bandwidth allocation, smart packet forwarding and advanced compression technologies. While compression created more bandwidth, dynamic bandwidth allocation and smart packet forwarding ensured that critical applications would always obtain the bandwidth required to meet performance requirements, whatever the network condition. The combination of these two technologies dramatically improved application performance without the need to implement bandwidth upgrades. The realization of such technology ensured that different classes of traffic emerged. It also made sure that the network architecture could identify and discriminate against different classes of traffic. This discriminatory characteristic formed the central, guiding tenet of a new intelligent network mechanism implemented by service providers.

4.2 Quality of Service (QoS) and Structured Extensibility Frameworks

Quality of Service (QoS) is the primary control mechanism implemented under the intelligent network model by service providers. The term refers to a broad collection of networking technologies and techniques designed to provide guarantees on the ability of a network to deliver predictable results. On the Internet and in other networks, QoS is the mechanism that ensures that transmission rates, error rates and other characteristics can be measured, improved, and, to some extent, guaranteed in advance (Crawley, Rajagopalan and Sandick, 1998). QoS therefore functions as a mechanism that defines the level of performance in specific applications. It is a feature that prioritizes and guarantees bandwidth for selected applications to achieve optimal service performance.

QoS ensures that priority is assigned to specified data, transiting specific routes, including mobile and other ubiquitous devices. By assigning QoS levels to electronic network traffic flows, devices can get all the required bandwidth and network priority demanded by specific applications (Crawley, Rajagopalan and Sandick, 1998). With the continuing emergence and importance of demanding, high-priority applications such as online financial and currency trading, the implementation of intermediary QoS technology upon public electronic networks became critical.

QoS allows traffic on public network infrastructure to be managed in such a way so that it can be strictly governed and monitored and have consistent quality. QoS is therefore described as a set of techniques that acts to efficiently manage network resources for business use. The mechanism is a key component of new network designs that have emerged to exercise a greater degree of control over the Internet. Since end-to-

end infrastructure did not guarantee a dedicated level of network service, the original Internet architecture did not assure any specific transmission rates or performance.

End-to-end architecture only endeavors to provide best effort service. Under that model, the network did not provide any special features to recover lost or corrupted data. Recovery services were instead supposed to be provided by applications in end systems. By removing the need to provide recovery services, the network was deemed by its original designers to operate more efficiently. The years immediately following the commercialization of the Internet however witnessed rapid growth rates in network traffic. As a result, network administrators have needed to keep pace with increasing usage demands by continually adding capacity to keep up with the popularity of new resource-demanding, mission-critical business applications.

The QoS mechanism provides a set of tools that allows network administrators to manage such conditions, by exerting new controls over network resources. The new tools improve service to mission critical applications and users, while simultaneously stemming the rate at which capacity must be increased. QoS therefore improves service to network users while reducing the costs of providing these services (Crawley, Rajagopalan and Sandick, 1998). QoS also makes it possible for a service provider to offer service differentiation to customers, where service expectations are linked to the amount paid for the service. It works to form one of the bases by which traffic congestion can be managed, while working symbiotically with the service provider's desire to differentiate product offerings to its customers. Under the QoS model, a network can be segmented into a number of performance levels, with access priced at

each level. Quality of Service therefore functions as a "tiering" mechanism that is determined by the network operator.

Often, QoS mechanisms are designed to prioritize traffic so that only one centralized data store is required to manage and direct network resources. As network engineers recognize, QoS in the simplest sense means providing consistent, predictable data delivery service and satisfying customer application requirements from a centralized control point. To enable QoS requires the cooperation of all network layers from top-to-bottom, as well as every network element.

The open end-to-end network model, in contrast, ensures that any user can implement any service or device upon the network without top-down co-ordination. Open network design, as defined by communication professor Dwayne Winseck (1998), is a model in which the constituent components, functions and services of telecom networks were separated, thereby unbundling network services from general tariffs and requiring that separate aspects be made available to all on an as needed basis. In theory, open networks attempt to limit the control of telecom networks by service providers that historically refused network interconnection to competitors, offered services on an all of nothing basis, and denied access to network functions required by competitors (Winseck, 1998: 26). Winseck thus states that open network protocols limit the scope of network monopolies by allowing interconnection and delineating services that are to be available according to commercial criteria versus terms defined by regulation. The QoS mechanism, in contrast, enforces service regulation through technology and ensures limitation of unfettered user access to all network resources by placing priority on

selected data transmissions. As a result, only innovations introduced by the broadband provider can be introduced on a QoS-based network.

QoS involves a broad range of technologies, architecture and protocols that have evolved over time. It was developed as a method to progress the original Internet design devised by Cerf and Kahn (1974) towards greater control over data packets. One of the first attempts to give priority to data packets that traversed Internet compliant networks was a protocol known as IEEE-802.IP, or user priority field (Blight and Hamada, 1999). This protocol involved the addition of a user priority field to local area network packet headers. The three-bit field gave eight levels of priority. Traffic classes could be assigned priority fields, with high priority traffic classes shifting any side effects of an overloaded switch or router onto the traffic classes with lowest priority. However, if the load from all traffic classes of elevated priority was so great that it in itself exceeded the entire capacity of the switch or router, then all other classes would be denied access altogether, and even the priority class traffic would suffer service degradation. To counter this problem required a more complex solution than 802.IP, and more of an architectural solution that considered the entire network (Blight and Hamada, 1999).

In order to exercise more control over data streams, network engineers developed Class of Service (CoS), technically referred as 802.IP Layer 2 Tagging. CoS was a method of managing traffic in a network by grouping similar types of traffic (for example, electronic mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority (Blight and Hamada, 1999). CoS was a queuing discipline. The algorithm was designed to compare

fields of packets, and to classify packets in different priority queues. Class of Service attempted to introduce full QoS principles into Internet protocol through defining the type of service or TOS field. TOS, once again utilized a simple priority field, but one that was actually integrated into the data packet, rather than added onto the packet as an appendage (Blight and Hamada, 1999). TOS was never utilized on a large scale since Class of Service technologies did not guarantee a level of service in terms of bandwidth and delivery time. It only offered "best-effort" and as a result was not widely adopted for high-bandwidth, mission-critical applications.

The simple priority field methods (IEEE-802.IP and TOS), though useful in simple networks where congestion was not a major issue, did have shortfalls, and alone were not satisfactory for large and complex networks carrying large volumes of traffic of varying types. To properly support real-time business applications, it was necessary to develop an architecture that actively controlled traffic entering a network and the switches and routers in that network. The two methods that were developed to control these were entitled Integrated Services (IntServ) and Differentiated Services (DiffServ). The latter method would become the standard model for the QoS mechanism.

Integrated Services essentially defined a continuous pathway through a network for each application's data packets. IntServ achieved this by using the Resource Reservation Protocol (RSVP), which worked to dynamically maintain a path for each application's packets through a network, using the resources (network switches) with the lightest load. This state was maintained as a flow with an associated policy for admitting

traffic to the network, and pre-determined packet handling characteristics at each data hop (Braden, Clark and Shenker, 1994).

The IntServ methodology was found to be complex and too demanding of processing requirements in network switches, so most network providers preferred to use the differentiated services model. In the DiffServ model, traffic is classified into flow, although per flow resource reservation is not required (Braden, Zhang, Berson, Herzog and Jamin, 1997). The IP packets are marked, using a DiffServ field. This field uses the same bits or classification as a TOS field, although each bit has a different meaning. The fundamental advance provided by DiffServ, over and above TOS is that it applied an admission control mechanism at the entry point of a network. At the entry point, a network switch would determine the service to be applied to packets and the amount of traffic admitted within each service class (Braden, Zhang, Berson, Herzog and Jamin, 1997). Typically, DiffServ works to classify traffic entering into a network into flows. At the entry to the network, a policy is applied to the classified flows. This shapes the traffic to meet the requirements of the particular flow. If excessive traffic enters the network, then packets in the low priority flows are discarded. The shaped traffic is then assigned a particular behaviour aggregate. The IP header DiffServ field is marked with the appropriate DiffServ Code Point (DSCP). When it is passed through a DiffServ network, the DSCP triggers a selected per-hop behaviour from the interior of the network (Braden, Zhang, Berson, Herzog and Jamin, 1997).

For a network to support DiffServ, every switch or router in the network must be able to respond to the service marking contained in the packet's DSCP, and to respond

consistently with this DSCP. No further classification or profiling is required or performed inside the network. In this way the most intensive classification and profiling of traffic can occur at the edge of the network, though the core still defines and determines what data can ingress. The ability to classify traffic, apply policies and traffic shaping, and priority mark packets is central to the QoS mechanism, along with permitting the core to support DSCP classification and priority treatment. RSVP also had the ability to identify specific users and specify QoS priority services such as multimedia.

Queue management is also fundamental to QoS. It enables bandwidth control (which is essentially admission control), and ensures that traffic is dealt with as its priority required (Allied Telesyn, 2003). To achieve this, two main queue types are required: weighted fair bandwidth distribution and priority. Weighted distribution allocated bandwidth to applications based on their needs, and thereby set maximum and minimum bandwidth limits. It ensured that applications with lower priority, for instance, could not absorb bandwidth allocated for other applications. Priority ensured that high priority traffic was always given priority over other traffic, and thereby suffered less delay. It did this by dropping lower priority packets through a random early discard mechanism. When server congestions occurred, the QoS mechanism dropped progressively more and higher priority packets, until congestion was eased (Allied Telesyn, 2003).

Nortel Networks, one of the leading manufacturers of advanced Internet technologies, developed an entire approach to networking revolving around QoS in the late 1990s (Nortel Networks, 1999). The policy management system allowed a service

provider to dictate access rights and use, based on the established profile of the application, user and usage group. Nortel's comprehensive policy management solutions focused on access provision, policy definition and enforcement and user verification, and were essentially deployed to ensure QoS (bandwidth, latency, priority) and security (authentication, authorization and auditing). The system achieved these dual goals by maintaining, enforcing and coordinating policies from the network core (Nortel Networks, 1999). Using a centralized "advanced directory" model, a service provider or enterprise could define policies, user information, network configuration data and network addresses from one main location. This centralized data store was able to assign priority to defined business traffic. Also ingrained into the system was enhanced network surveillance. Under the policy management model, a framework was provided that allowed network managers to: define policies for prioritization and access on the network; enforce policies during network operation by interacting with application and user request for priority or access; and verify policy compliance through ongoing monitoring of service level performance (Nortel Networks, 1999).

Another noted Internet technology company, Cisco Systems, also specialized in providing QoS to corporate customers and service providers through its specialized routing software. Cisco's Internetwork Operating System (IOS) software utilized multiple QoS-related protocols to classify and mark data packets, reduce and manage data traffic congestion and specifically condition traffic for such management (Cisco Systems, 2001). The system allowed service providers to isolate network traffic by the type of application and computing appliance, even down to specific brands, interfaces

used, user type, individual user identification and site address. IOS software also functioned to impose admission control and policing in order to develop and enforce traffic policies. These controls permitted the limitation of traffic flowing into a network and allowed for policy-based determinations on whether a network would support the requirements of incoming applications. Cisco integrated edge function control into software so that enterprises and service providers could deal with each subscriber as an individual entity, assigning access authorizations, bandwidth allocations and security filters for each address (Cisco Systems, 2001). The Cisco system also worked to allocate and reserve bandwidth and speed for specific applications. Utilizing the Resource Reservation Protocol (RSVP), an integral QoS mechanism, Cisco's system could make bandwidth reservations for high-demand content such as video (Cisco Systems, 2001). Cisco software also defined a committed access rate (CAR), which allowed system administrators to specify the user access speed of any given data packet by allocating the bandwidth it received, based upon its IP address, application, precedence, data port or even network adapter specification (Cisco Systems, 2001). This feature not only imposed control, but also allowed service providers to impose modes of network surveillance.

Network surveillance was important as more measurable criteria in conjunction with guaranteed transmission rates meant service providers could offer more products and services to their customers at premium rates. As a result, all major service providers adopted technologies and techniques to implement QoS in order to measure and monitor Internet performance. Most implemented QoS policies and policy servers. The industry

standard QoS policy model defined policy enforcement points (PEPs) and policy decision points (PDPs). PEPs included routers, switches and other devices that were able to act as admission control agents. Typically, PEPs worked together with PDPs to apply the network administrator's QoS policies. PDPs provided the higher layer intelligence required to process abstract policies. PDPs reviewed RSVP signaling messages that arrived at various PEPs and decided whether or not the corresponding traffic could be admitted to a network. PDPs also used top-down provisioning to push to PEPs configuration information regarding non-signaled traffic flows from the centre of the network to the edge (Strassner, 2004).

The adoption rate of QoS technologies increased exponentially as broadband networks began to be widely deployed in the late 1990s for the explicit use of business. With the rise of the network economy, enterprises needed to coordinate their operations on a global scale. QoS guaranteed network reliability so global business data could be prioritized. The technology was incorporated into network routers at peering points, or major Internet junctions, to ensure that prioritized corporate traffic on different network backbones could be differentiated. Once employed, the technology allowed traffic to be controlled based on price, geography, size, performance, ownership and access rights. While an "end-to-end" infrastructure would allow access to the full suite of IP services inherently available with regular, narrowband Internet access, the QoS-driven intelligent network integrated into broadband access would require special authentication from the service provider for its users to access the entire IP suite. As a result, administrators of the network would have full control to set policies based on user class. Those enterprises

that paid a higher fee, would be guaranteed bandwidth performance, while those that paid a lower fee would be limited to lower data transfer speeds. This type of service discrimination is observed when differentials in commercial and residential broadband services are considered. Residential customers typically had lower access rates, and were not able to connect their own content or electronic mail servers to a broadband Internet service provider due to technical restrictions. Commercial customers, on the other hand, typically have faster access rates with no restrictions, permitting them to deploy a wider array of services, as long as they are specifically paying a premium to do so. As Bar *et al.* (2000) note, the integration of Internet access and carrier capacity allowed for service providers to control all facets of network access in its entirety. Consequently, administrators of the QoS mechanism could block access to certain users based on geography, or could block access to certain network resources (such as Web sites or video) based on where the users logs into the network, or who the user is. The QoS mechanism even had the ability to discriminate amongst multiple user classes, meaning that certain corporate users designated as "high priority" such as executives, would gain access to better services and faster broadband data rates, in comparison to lower-level staff.

QoS also allowed enterprises to make decisions based on size, or economies of scale. The mechanism permitted bandwidth control for specific sites: allowing corporate management to make network access faster at specific, distinct geographic locations. The characteristics of the QoS mechanism therefore allowed corporations to determine access by setting specific policies. By employing QoS, enterprises improved access to their

information resources and improved their performance. Due to the proliferation of commercial applications, enterprises wanted to monitor and control their network traffic and prioritize the status of their applications. The QoS mechanism enabled enterprises to obtain highly differentiated services and quality levels for those applications. QoS allowed for the identification and isolation of different types of network traffic and also enforced admission control and network policing.

The mechanism also gave network operators the option for the preferential queuing of specific traffic such as hypertext, telephony, video and electronic mail. Consequently, the technology permitted service providers to implement strategies that allowed them to exercise control over the evolution of electronic networks. Equipment manufacturers, such as Cisco Systems and Nortel Networks addressed the growing desire by telecommunication operators to control networks, by designing network routing devices that place intelligence and resources such as QoS into the network and under the control of network owners. The result is that telecommunication networks have the technical ability to filter their networks for content and tier their networks on the basis of speed.

Blocking content is an ostensive example of using a QoS-based routing system to exercise enhanced control over networks. In July 2005, Canadian telecommunication firm Telus blocked access to a Web site supporting the company's labour union on its network during a dispute, as well as over 600 other Web sites, for approximately sixteen hours (CBC, 2005). In April 2006, America Online, a large Internet service provider, blocked all incoming customer e-mail that mentioned an advocacy campaign opposing

the company pay-to-send an e-mail scheme (ZDNet, 2006). And recently, customers of both Rogers Cable and Bell Canada have speculated that both firms have begun to block access to peer-to-peer networking services such as BitTorrent. Though Rogers denies that it specifically blocks this service, it does admit that its use QoS to prioritize its customers' network traffic (Geist, 2005).

In terms of access, all communication firms that offer broadband service use QoS-based systems to determine speed limits. Though the connection that brings Internet access to a home can typically reach six megabits per second, often service providers will arbitrarily limit speeds to four megabits per second in order to offer both a basic service and an advanced service. Shaw Cable, a Canadian communication firm, even offers a premium QoS upgrade for its broadband service to enhance third-party VoIP services used on its network (Shaw, 2005).

In terms of business customers, communication firms provide routing devices and high-speed lines that enable Metro Ethernet systems, allowing businesses to access wide area, private networks on a priority basis. All Fortune 500 companies employ such systems to improve communications between head and branch offices. They can also take advantage of these systems to filter in-bound and out-bound content based upon their own corporate policies. Through Metro Ethernet networks powered by QoS-based routing equipment, corporations can also execute traffic shaping to ensure that specific traffic such as VoIP and Web casting is given priority.

As a result of these new network interventions, the open network architectures of the Internet are being severely challenged by closed network designs that enhance the

service providers' ability to allocate bandwidth, resources, speed to various classes of network traffic and information and services based on their relation to the network owner, revenue potential, class of user served, and judgments regarding content quality.

The business intelligence metrics available through a QoS interface includes availability, performance, resource utilization, capacity planning, and application usability. These tools allow telecommunication providers and network operators to measure network usage to enhance their network's return-on-investment. The use of QoS allows service providers to concurrently prioritize network traffic and applications while quantifying network traffic to increase revenue. As a result, classes of network use emerge that can be delineated on the basis of identity, geography, service performance, and prioritized on the ability to pay for differentiated services. Frequently, it is noted in literature concerning QoS that it is possible to assign valuable service priority during transmission (Cisco Systems, 1999a, 1999b, 2000). Value in the case of the QoS communication service model is assigned by the service provider, which allows it to set different economic values amongst its different type of customers. The business model promoted by Cisco Systems, Nortel Networks, and other telecommunication equipment manufacturers, thus allows service providers to generate revenue by defining and billing for differentiated services targeted to specific customer requirements. When new applications emerge, service providers can capitalize upon their deployment, by monitoring network usage and charging for new services. Accordingly, QoS is noted in marketing literature as a mechanism that allows network operators to optimize profits by

offering differentiated services to premium customers ready to pay for superior network performance (Cisco Systems, 1999a, 1999b).

The differentiated service capacity is interwoven into the technological design of the hubs of the network architectures, such as servers and routers. The differentiated service capacity allows administrators to i) specify policies that establish traffic classes and service levels; ii) define how new resources are allocated and controlled to handle traffic classes; iii) efficiently map packets into the traffic classes; iv) apply policies to meet application and security requirements; and v) collect and export detailed network traffic and service allocation statistics, in order to assign prices for services (Cisco Systems, 2000).

Due to the options outlined above, all major global service providers by 2005 had widely adopted and deployed technologies with QoS mechanisms, in effect to integrate a pay-per capacity into their networks. According to Mosco (1989: 124), the essence of computer communications systems is to "measure and monitor information transactions for control and profit." The QoS mechanism provided the tools for service providers to translate the pay-per capability that Mosco defined into Internet-based architecture. As a result, Cisco Systems' fiscal year-end reporting for 2001 indicated that a wide roster of major services provider customers, including Qwest, America Online (AOL), France Telecom and China Telecom had all opted for QoS-enabled router technologies (Cisco Systems, 2001). Nortel Networks in 2001 had also supplied QoS-enabled technologies to major service providers such as Bell Canada and Sprint (Nortel Networks, 2001).

As Mulgan (1991) outlined, the development and use of such control technologies ultimately lead to their heightened utilization and refinement. This fact was illustrated in early 2003, when Nortel Networks unveiled a bundle of enhanced QoS technologies entitled "advanced business connectivity" which was designed to provide a consistent experience for business users, "whether sitting at a desk at the company headquarters, at a customer site, or via an Internet kiosk at an airport" (Nortel Networks, 2003). The experience was designed to remain consistent regardless of the type of device used to access the network, be it a company-issued computer, a Web-enabled cell phone, or a browser accessed from a remote location. Business applications under this scheme were secure and scalable, and able to quickly adapt to the business cycles of enterprise. By employing such schemes, service providers were able to offer both the public and private sectors higher levels of differentiated services in order to support new frameworks of "structured extensibility".

Structured extensibility extended networks by integrating a broad range of technologies into a highly integrated network of economic relationships. The network logic was predicated upon the emergence of information grids that were in turn, based upon distributed and ubiquitous computing facilities that connected industries and markets, concurrently increasing the rate of corporate expansion. According to Aradaiz, Freitag and Navarro (2000), ubiquitous computing is a paradigm in which networked computing resources are extended beyond traditional conceptions of computing. Users augment their computing and communication capabilities with a multitude of computing devices, conceivably allowing the network to become an infinitely accessible

environment for those specific users. Resources are mobile and have both wire-based and wireless connectivity. In such a scenario, computer services and devices make use of information processing that can be easily obtained through nearly any microprocessor-based device. The value proposition of structured extensibility is thus predicated upon the omni-presence of computers, consumer electronics, sensors and computerized networks. The wide and growing use of computers that are embedded within and intrinsically part of a larger collection of devices leads to a metamorphosis in human perception in which computers are not seen or used as distinct machines on a distinct single network. Instead, computers are implanted into a wide array of everyday devices, such as telephones, cars, microwave ovens, cash registered, personal digital assistants (PDAs) and multitude of other fanciful and mundane devices and systems. All of these devices are bound together by a broad range of communication technologies – including the Internet and wire-line and wireless telecommunication links, providing the infrastructure necessary for the devices to be tools of greater economic integration. The process of structured extensibility allows all these devices to seamlessly interact, creating new technological arrangements, in which information is created and interchanged.

This new framework leverages Web services, which are technologies that are designed to offer consumers a greater level of interactivity through a network of ubiquitous devices. Web services make interactive application functionality available over the Internet in a standardized, programmatic manner. Applications that could not be accessed except by following rigid, traditional computing approaches were made accessible using the same infrastructure that had enabled the widespread use of Web

technologies. The result was that enhanced Internet services were not restrained to computing devices. A new generation of Internet services, based upon Web services, extended commercial and financial services to a wide host of consumer electronic devices, including set-top cable and satellite boxes, and even household appliances and miniature sensors. These devices interacted with each other, regardless of their function, and the platforms that they were developed in. Web services therefore created high levels of interoperability and interconnection between seemingly disparate devices. For this reason, many computing and telecommunication industry participants defined Web services as an entirely new breed of Web application. Industry analysts described Web services as a group of closely related, emerging technologies that describe a service-oriented, component-based application architecture that is based on an Internet-centric infrastructure. Web services thus represented a new model in which discrete tasks were distributed widely throughout a value net.

Web services are distributed components that can be combined to form unique business processes. According to an IBM (2001) technical brief on the subject: "Web services are self-contained, self-describing, modular applications that can be published, located, and invoked across the Web. Web services perform functions, which can be anything from simple requests to complicated business processes. Once a Web service is deployed, other applications (and other Web services) can discover and invoke the deployed service." Microsoft similarly defines Web services as applications delivered as a service that can be integrated with other Web services using Internet standards. The

firm defines Web services as "programmable application logic, accessible using standard Internet protocols" (Microsoft, 2001).

For the Web services/structured extensibility model to operate efficiently, especially for demanding applications that involved the co-ordination of huge amounts of data or interactive content such as audio and video, guarantees in service performance are required. QoS is used to provide that service guarantee. Many real-time business applications based on the structured extensibility model are intolerant of delay, and as a result, QoS is designated as an essential feature for electronic data transmission and mobile data interaction and exchange by enterprise.

4.3 Centralized Network Resources

Though QoS is an essential component for the implementation of distributed knowledge systems, centralization of network resources is still equally beneficial when implementing business applications, since centralization creates easier-to-enforce, uniform standards. Network resources that are centralized allow enforcement of specific access and resource policies and minimize application diversity by restricting interconnection options. Reducing diversity of node configurations at the ends of the network simplifies the task of keeping resources upon the network as homogenous as possible. In addition, resources such as files, servers and applications, when kept in a central location, can be protected from unauthorized modifications. The protection and relative isolation of centralized resources reduce the chance of deletion, corruption, or compromise of resources critical to business applications, thereby mitigating risk and

uncertainty. The centralization of network resources also permits enhanced monitoring and control. While distributed, end-to-end infrastructures diffuse network utilization and encourages innovation due to ease of interconnection, it also makes it much more difficult to enforce configuration standards and maintain control over access. By placing network resources in a few centralized locations instead, network operators are able to regain control over the configuration of the network itself.

Centralized control over network configuration means that service providers can exercise full power over the allocation of network resources. This approach, in effect, reduces competition and limits user choice on what resources users can themselves deploy. Centralizing resources in the context of Internet service is quite paradoxical, since the original intent of the open, inter-networked system was to develop a widely diffused and distributed architecture, where network resources could be freely deployed. The new intermediary approach however favours the enclosure of network resources that technically had operated at the network periphery. An example of such enclosure is the development of centralized server farms and peering points. While it is technically feasible to operate Internet servers at the edge of the network for business purposes, service providers are increasingly opting to centralize Internet servers in special facilities. As a result, entire lines of business have emerged that focus on providing centralized, outsourced Internet services.

Outsourcing can be defined as "the strategic use of outside resources to perform activities traditionally handled by internal staff and resources." (Outsourcing Institute, 2001). Sometimes referred to as facilities or supply chain management, outsourcing is a

strategy by which an organization "contracts out" major functions to specialized, external service providers, who become supply-chain business partners. Information technology outsourcing consists of third-party provision of products, services, capabilities and skills. The main drivers for outsourcing IT infrastructure are to reduce costs and gain access to technical capabilities and support. Many firms justify the use of outsourcing because it allows them to focus on their core business competencies. Since IT is not seen as the core competence for many companies, they reason that information-processing capacity can be outsourced to a third party without incurring any loss in overall business performance. Corporate managers purport that outsourcing gives them more time to concentrate on more pressing business issues. Further, many companies, on average, experience a costs savings and increases in capacity and productivity due to outsourcing. For this reason, outsourcing has become an extremely popular business option. Gartner (1999), an IT research consultancy, estimates that the IT outsourcing market in North America grew from $101 billion in 2000 to $160 billion in 2005 as corporations and government agencies tried to lower IT spending and focus their resources elsewhere. With the ability to externalize IT functions, many businesses now perceive information technology as something separate from other business processes and activities. As a result, many organizations now treat IT as a commodity that is readily accessible in the marketplace. This approach toward information technology has greatly influenced the implementation of new information and communication systems. IT systems as a consequence are now primarily adopting and utilizing new infrastructure models that externalize information resources and integrate business processes. The primary

emphasis of the new architecture is to: i) establish new marketplaces through networks; ii) introduce and implement technical, functional and corporate convergence; and iii) exercise high degrees of control over business processes. This approach to infrastructure deviates from original IT system architectures that emphasized the internalization of resources at the edge of the network. The approach creates new economies based on network transactions, which has transformed network usage and service provision. With networks now primarily conceptualized as economies, Internet architectures have become centralized and hence highly controlled and measurable. Control is better achieved through centralization since IT resources are located in telecom facilities rather than at corporate locations.

IT outsourcing establishes new marketplaces by utilizing business partners, mainly service providers, to complete tasks or maintain resources that traditionally would be maintained by an organization internally. By extricating information technology services, corporations and governments achieve cost-savings by reducing expenditures related to implementing and maintaining new technologies. Service providers eliminate the need for organizations to maintain software applications, technology facilities and the associated staff required to maintain such systems. The most notable service providers are those that specialize in implementing electronic business processes. With e-business, organizations can sell and fulfill products and services to their customers electronically. Electronic business systems also enable collaborative commerce between organizations, transforming supply chains into one intelligible framework that seamlessly integrates commerce applications, from supplier to customer. A main objective of enterprise IT

outsourcing therefore is to utilize information and communication technologies to co-ordinate and integrate separate business processes. Technology architectures associated with outsourcing e-business processes include business process outsourcing, application service provision, software as a service and Web hosting.

Business process outsourcing (BPO) is the contracting of a specific business task to a third-party service provider. Usually, BPO is implemented as a cost-saving measure for tasks that a company requires but does not depend upon to maintain their position in the marketplace. BPO is often divided into two categories: back office outsourcing which includes internal business functions such as billing or purchasing, and front office outsourcing which includes customer-related services such as marketing or technical support.

BPO services use both technology and "global labour arbitrage" to affect cost savings for large corporations. A majority of BPO vendors are located in developing regions such as India, China and Latin America, and utilize Internet-based structured extensibility models to deliver their services to companies in North America and Europe. Leading companies providing BPO services include Accenture, Siemens Information Systems, Unisys and Wipro Technologies. Forrester Research (2003) expects that the BPO sector will grow to $146 billion by 2008.

Application service provision allows individual organizations to lease specific software and utilize it via the Web, rather than purchase the software for installation within the enterprise. Application services range from word processing and accounting software packages to chain supply management and data warehousing. These services

enable governments and business to use the most recent technology without assuming total cost of ownership or full administrative responsibilities. These services are provided by application service providers (ASPs), companies that offer business access to computer programs over the Internet, which otherwise would have been located on the business premises. Occasionally referred to as "apps-on-tap", application service providers distribute IT resources over spatially diverse geographies. ASPs often own, operate and maintain both the software and servers that transmit business software. The service providers are primarily independent and vendor-natural. As a result, there are thousands of ASPs that provide a myriad of different applications targeted at multiple markets. Market research estimates that ASP revenues increased from $986 million in 2000 to almost $5 billion in 2005 (IDC, 2005).

Notable ASPs include Doubleclick, an Internet advertising service and Ariba, an automated electronic procurement manager. Such service providers make their applications available via the Internet. The providers usually bill for the usage of the application on a pay-per use basis.

Larger vendors have extended this popular approach to software provision through a delivery model entitled Software as a Service (SaaS). SaaS differs from the ASP model only in that application delivery is typically closer to a one-to-many model (single instance, multi-tenant architecture) than to a one-to-one model for all clients. Prominent firms that offer SaaS include Microsoft and Google, who offer collaborative office software, and Saleforce.com which provides on-demand customer relationship management solutions.

Market research verifies the rapid escalation in enterprise demand for SaaS. In May 2004, research consultancy Summit Strategies found 31 percent of large U.S. companies with more than 1,000 employees were using SaaS, and an additional 11 percent were in the process of evaluating SaaS offerings (Summit Strategies, 2004). In May 2005, AMR found that 40 percent of all U.S. companies use hosted applications, and estimated that 49 percent would use them within the next 12 months (AMR, 2005). Gartner (2005) forecasts large companies will fulfill 25 percent of their application demands with hosted software by 2010.

Forrester Research predicts the market for traditional on-premise enterprise applications will only grow four percent through 2008 (Forrester Research, 2005). By comparison, IDC predicts the SaaS market will grow at a 21 percent compound annual growth rate, reaching $10.7 billion worldwide in 2009 (IDC, 2005a).

Major growth is also expected in the outsourced Internet services market. Spending on Web hosting is predicted to exceed $13.5 billion by 2007 (Insight Research, 2002). Web hosting is the term used to describe the basic service of providing power, bandwidth, air-conditioned computer room space, and rack space for servers at a centralized network facility. Providers that offer this service are said to "host" these Internet servers, which typically come from organizations that wish to rent that space outside of their private corporate data centre. These services can be provided on a collocation basis, where the customer manages servers, or they can be provided as an outsourced managed service, where the service provider takes responsibility for the servers, the server site, and other ancillary functions.

Companies that provide advanced Web hosting services include all telecommunications firms, including AT&T and Bell Canada; large computing firms such as IBM; and pure-play IT networking carriers such as Savvis. These firms locate their data centre facilities at core network junctions. By locating Web hosting services within Internet nodes at the centre rather than at the edge of the network, organizations place and access their intelligence through an intermediary.

The premise behind providing such services is to improve levels of service quality. Through centralized resources, service providers argue that users, especially corporate customers, experience fewer disruptions and more timely service. With services fixed at a specific location, less staff is required to maintain network resources. Costs are controlled since major repairs only need to be made in centralized facilities.

Centralized facilities, entitled data centres, as a result have become the *de rigueur* architectural model for service providers. The facilities incorporate network operation centres, which act as the master control mechanisms for outsourced server operations. The network operations centre consists of all the infrastructure, equipment and personnel necessary to provide business consumers with first-class Internet connectivity. All first-tier providers and major telecommunications companies build them to create the physical environment necessary to keep their business clients connected to high-speed Internet trunk connections 24 hours a day, seven days a week. Network operations centres, or NOCs as they are commonly referred to, are expensive, world-class facilities. They are located in major metropolitan centres throughout the United States, Canada, and Europe and are designed to provide the widest range of security, reliability and speed. NOCs

usually have multiple connections to high-speed, first-tier T1, T3, or OC-3 bandwidth connections. These connections are referred to as first-tier, because they are the raw pipes that contain the majority of Internet traffic. Traffic at these points are interconnected, or peered, with one another, allowing for the exchange of data across multiple networks. At these peering points, service providers and corporate customers can monitor, classify, prioritize and even filter traffic through QoS-based network switches and routers. Corporate customers are able to leverage these facilities in order to locate their servers in these network junctions and obtain the highest levels of control over network resources without the resources being physically located on their property. Network resources include financial and trading applications as outlined in the first chapter of this thesis, which require an elevated level of connectivity, equipment redundancy, control and risk mitigation.

Chapter 5 Conclusion

Corporate imperatives have played a major role in driving the imposition and implementation of new control technologies upon electronic networks. Emerging frameworks of structured extensibility and global finance have placed pressure on service providers to offer more secure environments to their clientele. The consequence is that service providers have attempted to re-exercise monopoly status over network resources through technology. Using mechanisms such as Quality of Service (QoS) and server centralization, service providers have deployed technical strategies to reduce risk and provide more control to enterprises. Oversight technologies respond to businesses' desire to mitigate the uncertainty and risk generated by the new abundance of information and technology. While neoclassical economists argue that new technologies can facilitate marketplaces of perfect information (Stiglitz, 1985), a situation in which all data relevant to a problem is known and can be theoretically collated and applied, they exclude from consideration the fundamental risk and uncertainty that emerges from the conditions of continual changes in technology and the exponential growth of information (Winseck, 1995).

Mulgan (1991) notes that the continuous generation of information creates a *paradox of control*. He theorizes that as the number of network connections increase and as the speed of communication rises, then the predictability and controllability of communication systems decreases. Increasing information flows therefore result in greater societal uncertainty. Information abundance, especially in emerging technological and financial network environments upon which enterprises depend for

global trade, encourage organizations and service providers to exercise greater control over such environments.

Consequently, as institutions, economies and societies grow increasingly complex, their costs of co-ordination and control tend to rise faster than their material capacities. The resultant investment in control mechanisms therefore brings about their proliferation. Communication scholar Neil Postman reaches the same conclusion. He notes that an increased supply of information creates more demand for control. For Postman (1993, 72):

> The relationship between information and the mechanism for its control is fairly simple to describe: Technology increases the available supply for information. As the supply is increased, control mechanisms are strained. Additional control mechanisms are needed to cope with new information.

Mulgan (1991) notes that control is ultimately not without cost; therefore the desire to control faces practical limits in application. The exact nature of the cost is tied into the social and economic environment in which the system operates. The social structure imposes a set of constraints on the exercise of the capacity for control inherent in the technological structure. Mulgan recognizes that technology imposes certain limits on the social organization of control and that both structures cannot be considered in isolation. Technology can thus create and foster a potential for control that may or may not be realized. It would inherently contain the capacity to control, but those with the capacity to employ it would have to elect to impose it. Technological control, as Mulgan defines it, is therefore exorable or flexible. It is subject to change and is not imposed automatically. This approach directly contrasts theories of control advanced by Beniger (1986) in which control is interpreted as inflexible. Technology is not simply pre-

determined to implement regimes of control. Instead, technology allows control to oscillate between different control models, societal groups and even philosophies.

In terms of networks, these philosophies oscillate between openness and enclosure. In terms of this study, technological models have been demonstrated to fluctuate between open, end-to-end and closed, end-to-intermediary infrastructures. Open architecture is propelled by libertarian elements in society seeking to impose horizontal control over network resources that would allow control by individuals and small businesses. Large corporations and governments support the closed architectures, to impose their own, self-serving vertical, monopolistic control over network elements. This thesis specifically examined this evolution and imposition of these control architectures upon electronic networks.

The open architecture, that first emerged during the embryonic stages of Internet design was a control mechanism that kept network protocols simple, computing and information processing at the edge of the network, and encouraged the greatest amount of interconnection. Individuals used the architecture to obtain unobstructed access to computer networks, which could be leveraged for interpersonal communication and even political action. In terms of small businesses, the open network architecture could be used to develop new innovations, including new information products and services that could be deployed and installed on the network without permission from the service provider. Typically, the open network architecture was made available through narrowband network operators, vis-à-vis dialup telephone access. This type of access

ensured that content and carriage were not intertwined; providing individual users at the network's edge the autonomy to communicate and innovate.

End-to-intermediary infrastructure, in contrast, bundled carriage with content. As a consequence, new broadband access technology, which includes cable and digital subscriber line (DSL), subjected users to new, enhanced modalities of control that restricts innovation and user autonomy. The new access technology leverages Quality of Service (QoS) mechanisms, which are employed to limit network usage based upon individual characteristics, and stop new innovative services from being deployed upon the network. The rationale for implementing the new technology was to provide business with more reliable service quality to provision capital and financial markets that were increasingly dependent upon electronic networks. With more and more transactions being conducted online, the financial industries demanded a guaranteed level of service. Guarantees could only be assured if a new reliable model was enacted, since the original open model only made a best effort concerning the transport of data. With the new intelligent network model, priority was assigned to specific types of data. Service providers as a result could profit by being able to charge corporate customers a premium to differentiate and prioritize their data above others.

This approach violates the tenets of original Internet design, but allows corporations to obtain dependable services for their business applications, which increasingly rely upon flexible frameworks that interface with ubiquitous computing devices and promote the global integration of multiple locales.

Such a shift from open to closed network infrastructures indicates that networks are indeed subject to evolution. Communication scholar Robert W. McChesney in conjunction with political scientist Edward S. Herman argue that in the 1990s, the Internet transformed from a participatory medium that served the interests of the public into being a broadcast medium where corporations delivered consumer-oriented information (McChesney and Herman, 1997). Winseck observed that "the evolution of new media is being biased away from the open systems model of telecommunications and the Internet towards a closed model, where in-house content is favoured over other sources, either in a heavy-handed manner, such as by refusing access to the network altogether ... or subtly through network design ... and so on in ways that give priority access to some sources of content and not others." (Winseck, 2003).

As a result, electronic networks cannot be characterized as either static or strictly open, benevolent environments that only promote greater interconnection of users or wider diffusion of markets. Subject to dialectics of control, electronic networks are dynamic environments that can be influenced by corporate power.

Mansell (1993) notes that an effective frame of reference for analyzing the strategic evolution of networks is a bifurcated model of control. Such an approach defines an "idealist" model, which is synonymous with a highly effective comparative market, and a "strategic" model, which is synonymous with market dominance and strong elements of monopoly or oligopoly. Mansell's approach underlines the fact that control is in a constant state of flux and that institutional factors and the exercise of economic and political power play a significant role in the selection of technological configurations.

The choice of technological configurations is divided between open and closed networking architectures. In terms of this thesis, the institutional factors that are examined are driven by corporate initiatives that influence the design process. Corporate choice impacts overall network design by embracing intelligent network technologies that limits access and shapes network traffic. This deliberate choice allows enterprise and service providers to exercise greater influence over network function. With intelligent networks, communication firms are able to obtain better control over the behaviour and activity of end-users. Communication firms and other large enterprises are also able to exercise greater control over network flows in terms of broadband guarantees, speeds, application priority, and traffic priority vis-à-vis technological intermediaries.

Using such systems as QoS and network centralization, corporations are able to obtain a higher level of structured extensibility, or global integration over their operational processes. Due to this benefit, corporations have influenced the technical development of networks away from open models, thus validating Mansell's notion of a design principle, which privileges human and organizational intentions for shifting the objectives of network development and control (Mansell, 1996).

In the political arena, arguments surrounding the design principle have crystallized in debates concerning network neutrality. Under such a principle, the network is ideally viewed as an environment that must be regulated in order to ensure the free flow of information and usage of applications. In terms of regulation, individuals and content providers have bounded together to lobby the U.S. government for the retention of end-to-end network designs. The preservation of end-to-end architectures

would mean that little obstruction to communication and innovation would be imposed on the network, thereby retaining the original environment that facilitated the initial growth of Internet-based electronic networks.

Large communication firms, in contrast, are advocating for the implementation of end-to-intermediary network designs. They argue that new innovative technologies challenge the integrity of their network infrastructures and that they should retain the rights to charge differentiated fees for access to their infrastructure. While no specific legislation has been passed concerning the application of network neutrality principles, the reality is that end-to-intermediary technologies have been installed and implemented by larger service providers.

As electronic networks have become pervasive throughout liberal-capitalist societies and used to co-ordinate economic transactions and global business functions, they are increasingly subject to regulation embedded into the actual hubs of networks. Service providers, who are primarily motivated by self-interest, embed policies into network architecture, allowing them to exercise greater control over online resources in order to stifle competitive network resources and increase profitability. As networks become more expansive, service providers exacerbate their deployment of technological intermediaries, thereby creating a cyclical, restrictive regime of control.

As open networks increasingly permitted greater opportunities for users to attach to decentralized and internationalized resources, service providers concurrently took strategic and calculated actions to exercise greater measures of control. The result was a fragmented, plural network environment that discriminated between classes of network

traffic, applications, and users. Such discrimination is the natural result of network evolution. While "end-to-end" network proponents claimed that networks could create an information commons that promote innovation, the reality was that networks were also concurrently mechanisms of control.

Mass communication scholars such as Mulgan (1991) and Mansell (1993) maintained that networks were methods to co-ordinate corporate and economic operations. With networks increasingly utilized to manage critical information and economic processes, primacy was placed on new modalities of control. These modalities included corporate-led regulation, enhanced surveillance capabilities and service provider-led network monopolization strategies.

Bibliography

Adorno, T.W. and M. Horkheimer. (1972). *Dialectic of Enlightenment*. New York: Continuum.

Ahuja, M. and K.M. Carley. (1998). "Network Structure in Virtual Organizations". *Journal of Computer Mediated Communication*, 3(4).

Alberts, D.S., and D.S. Papp. (1997), eds. *The Information Age: An Anthology on Its Impact and Consequences.* Washington DC: National Defense University.

Allied Telesyn. (2003). *QoS White Paper*. Available at: http://alliedtelesyn.com/corporate/media/whitepapers/qos_wp.pdf#search=%22QoS%20Allied%20Telesyn%22.

Ardaix, O., F. Freitag and L. Navarro. (2002). *On Service Deployment in Ubiquitous Computing*. Parallel Architectures and Compilation Techniques, PACT'01, Workshop on Ubiquitous Computing and Communications. November 2002; Barcelona, Spain.

Aron, R. (1961). *18 Lectures on Industrial Society*, trans. M.K. Bottomorw. London: Weidenfeld and Nicolson, 1967, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Aron, R. (1966). *The Industrial Society: Three Essays on Ideology and Development.* New York: Simon and Schuster, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Averitt, R.T. (1968). *The Dual Economy: The Economies of American Industry Structure*. New York: Norton, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Babe, R. (1994), ed. *Information and Communication in Economics*. London: Kluwer Academic Publishers.

Barrett, R. and P.P. Maglio. (1999). 'Intermediaries: An Approach to Manipulating Information Streams.' *IBM Systems Journal* 38(4), 629-641.

Bates, B. (1997). *The Macrosocial Impact of Communication Systems: Access, Bias, Control.* Available at: http://excellent.com.utk.edu/~bates/papers/93ica3.htm.

Beer, S.H. (1969). *British Politics in the Collectivist Age*. New York: Random House, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Bell, D. (1960). *The End of Ideology: On the Exhaustion of Political Ideas in the Fifties*. New York: Free Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Bell, D. (1973). *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. New York: Basic Books.

Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Berkeley, E.C. (1962). *The Computer Revolution*. Garden City, NY: Doubleday, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Bezold, C., ed. (1978). *Anticipatory Democracy: People in the Politics of the Future*. New York: Random House, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Blight, D.C. and T. Hamada. (1999). "Policy-Based Networking Architecture for QoS Internetworking in IP Management" in *IEEE Proceedings of Integrated Network Management VI, Distributed Management for the Networked Millennium*, 1999, 811-826.

Boulding, K. (1953). *The Organizational Revolution: A Study in the Ethics of Economic Organization*. New York: Harper, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Braden, R., L. Zhang, S. Berson, S. Herzog, S. Jamin (1997). *Resource Reservation Protocol*. Internet Engineering Task Force, Network Working Group, Request for Comments: 2205. Available at: http://www.ietf.org/rfc/rfc2205.txt.

Breed, W. (1971). *The Self-Guiding Society*. New York: Free Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Brock, G.W. (1994). *Telecommunication Policy for the Information Age: From Monopoly to Competition*. Cambridge: Harvard University Press.

Brown, L.R. (1972). *World Without Borders*. New York: Random House, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Cairncross, F. (1995). "Telecommunications: The Death of Distance," *Economist*, 30 Sept. 1995, 9.

Cahners In-Stat Group. (2000). *Internet Research Brief.* Available from: http://www.instat.com.

Carpenter, B.E. (1996). *Architectural Principles of the Internet.* Internet Engineering Task Force, Network Working Group, Request for Comments: 1958. Available at: http://www.ietf.org/rfc/rfc1958.txt.

Castells, M. (1989). *The Informational City: Information Technology, Economic Restructuring and the Urban-Regional Process.* Oxford: Blackwell.

CBC. (2005). *Telus cuts subscriber access to pro-union website*. Available at: http://www.cbc.ca/canada/story/2005/07/24/telus-sites050724.html.

Castells, M. (1996). *The Rise of the Network Society: The Information Age: Economy, Society and Culture.* Oxford: Blackwell.

Cerf, V., D. Clark, R. Kahn, L. Kleinrock, B. Leiner, D. Lynch, J. Postel, L. Roberts, and S. Wolff. (2003). A Brief History of the Internet. Available at: http://www.qazviniau.ac.ir/elearning/khorsand/module%201-%20internet%20architecture/lcc00%20Internet%20History.htm.

Cerf, V. and R. Kahn. (1974). "A Protocol for Packet Network Intercommunication" *IEEE Transactions on Communications*, 1974, 22(5), 637-648.

Cisco Systems (1999a). *New Revenue Opportunities for Cable Operators from Streaming Media Technology*. San Jose, CA.

Cisco Systems (1999b). *Control Your Network: A Must for Cable Operators*. San Jose, CA.

Cisco Systems (2000). *Cisco IOS Quality of Service*. San Jose, CA.

Cisco Systems (2001). *2001 Annual Report*. Available at: http://www.cisco.com/web/about/ac49/ac20/ac19/ar2001/index.html.

Clemmons, S. and S. J. Simon. (2001). "Control and Coordination in Global Electronic Research Planning (ERP) Configuration." *Business Process Management Journal*, 2001, 7(3), 205-215.

Collins, R. (1979). *The Credential Society: An Historical Sociology of Education and Stratification.* New York: Academic, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

ComScore Networks. (2006). *694 Million People Currently Use the Internet Worldwide According To ComScore Networks.* Available at: http://www.comscore.com/press/release.asp?press=849.

Crawley, E., B. Rajagopalan, and H. Sandick. (1998). *A Framework for QoS-based Routing in the Internet.* Internet Engineering Task Force, Network Working Group, Request for Comments: 2386. Available at: http://www.ietf.org/rfc/rfc2386.txt.

Daglish, R., (1972). *The Scientific and Technological Revolution: Social Effects and Prospects.* Moscow: Progress Publishers, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Dahrendorf, R. (1959). *Class and Class Conflict in an Industrial Society.* Stanford: Stanford University Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Dahrendorf, R. (1964). "Recent Changes in the Class Structure of European Societies". *Daedalus: Journal of the American Academy of Arts and Sciences.* Winter 1964, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Dertouzos, M. and J. Moses, eds. (1979). *The Computer Age: A Twenty-Year View.* Cambridge, MA: MIT Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Dizard, W.P. (1982). *The Coming Information Age: An Overview of Technology, Economics, and Politics.* New York: Longman, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Djlas, M. (1957). *The New Class: An Analysis of the Communist System.* New York: Praeger, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Dordick, H.S., H.G. Bradley and B. Nanus. (1981). *The Emerging Network Marketplace.* Norwood, NJ: Ablex, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Drucker, P.F. (1959). *Landmarks of Tomorrow.* New York: Harper and Row, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Drucker, P.F. (1969). *The Age of Discontinuity.* New York: Harper and Row, cited in

Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

van Dijk, J. (1999). *The Network Society, Social Aspects of New Media.* London: Sage.

Eisenstadt, S.N., ed. (1972). *Post-Traditional Societies.* New York: Norton, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Ellul, J. (1964). *The Technological Society*, trans. John Wilkinson. New York: Knopf, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Etzioni, A. (1968). *The Active Society: A Theory of Societal and Political Processes.* New York: Free Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Evans, L.B. (1977). "Impact of the Electronics Revolution on Industrial Process Control." *Science*, 1997, 195, 1146-1151, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Evans, C. (1979). *The Micro Millennium.* New York: Washington Square/Pocket Books, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

FCC Tariff 132; 1947 in [76] 13 FCC 2nd 420 at 437 (1968), cited in Brock (1994). *Telecommunication Policy for the Information Age: From Monopoly to Competition.* Cambridge: Harvard University Press.

Feurer, L.S. (1969). *Marx and the Intellectuals: A Set of Post-Ideological Essays.* Garden City, NY: Anchor Books, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Feenberg, A. (1995). *Alternative Modernity: The Technical Turn in Philosophy and Social Theory.* University of California Press, 1995.

Feenberg, A. (1992). "Subversive Rationalization: Technology, Power and Democracy," *Inquiry*, Sept./Dec. 1992, pp. 301-322.

Fiske, J. (1996). *Media matters: Race and Gender in U.S. Politics.* Minneapolis: University of Minnesota Press.

Forester, T., ed. (1980). *The Microelectronics Revolution.* Cambridge, MA: MIT Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Forouzan, B. (2003). *Data Communication and Networking (Third Edition).* New York: McGraw Hill.

Forrester Research. (2003). *Research Brief.* Available at: http://www.forrester.com.

Forrester Research. (2005). *Research Brief.* Available at: http://www.forrester.com.

Foucault, M. (1970). *The Order of Things: An Archaeology of the Human Sciences.* New York: Random House.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison.* New York: Pantheon Books.

Galbraith, J.K. (1967). *The New Industrial State.* Boston: Houghton Mifflin, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Gallie, D. (1978). *In Search of the New Working Class.* Cambridge: Cambridge University Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Galloway, A.R. (2004). *Protocol: How Control Exists After Decentralization.* Cambridge: MIT Press.

Gartner, A. and F. Riessman. (1974). *The Service Society and the Consumer Vanguard.* New York: Harper and Row, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Gartner. (1999). *Research Brief.* Available at: http://www.gartner.com.

Gandy, O.H. (1993). *The Panoptic Sort: A Political Economy of Personal Information.* Boulder, CO: Westview Press.

Geist, M. (2005). "Dangers in ISPs' bid for new tolls". *Toronto Star*, Dec. 19. 2005, Available at: http://geisttwotierinternet.notlong.com.

Giddens, A. (1984). *The Constitution of Society: Outline of the Theory of Structuration.* Cambridge: Polity Press.

Giddens, A. (1985). "Time, Space, and Regionalisation", in *Social Relations and Spatial Structures.* (Gregory and Urry, eds). New York: St. Martin's Press.

Gintis, H. (1970). "The New Working Class and Revolutionary Youth." *Continuum*, 1970, 8(1,2): 151-152, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Gouldner, A.W. (1979). *The Future of Intellectuals and the Rise of the New Class.* New York: Seabury Press, Continuum, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Gortz, A. (1968). *Strategy for Labor.* Boston: Beacon Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Gramsci, A. (1971). *Selections from the Prison Notebooks.* London: Lawrence & Wishart.

Gutstein, D. (1999). *E.con: How the Internet Undermines Democracy.* Toronto: Stoddart.

Halmos, P. (1970). *The Personal Society.* London: Constable, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Harvey, D. (1990). *The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change.* Oxford: Blackwell.

Hawkes, N. (1971). *The Computer Revolution.* New York: Dutton, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Herman, E.S. and R.W. McChesney. (1997). *The Global Media: The New Missionaries of Corporate Capitalism.* Washington, DC: Cassell.

Hiltz, S.R. and M. Turoff. (1978). *The Network Nation: Human Communication via Computer.* Reading, MA: Addison-Wesley, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

IBM. (2001). *Web Services Technical Brief.* Available at: http://www.redbooks.ibm.com/redbooks/SG246407.html.

IDC. (2005) *Research Brief.* Available at: http://www.idc.com.

Information Technology Association of America. (2003). *The U.S. Information Technology Industry: A Brief Overview.* Available at http://www.itaa.org.

International Engineering Consortium. (2005). *Intelligent Network: Definition and Overview.* Available at: http://www.iec.org/online/tutorials/in/.

Insight Research. (2002). *Research Brief.* Available at: http://www.insight-corp.com.

Internet Domain Survey. (2003). *Research Brief.* Available at: http://www.isc.org/index.pl?/ops/ds.

Internet Systems Consortium. (2005). *Domain Survey Information.* Available at: http://www.isc.org/index.pl?/ops/ds.

Ionescu,, G. (1976), ed. *The Political Thought of Saint-Simon.* Oxford: Oxford University Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Isenberg, D. (1997). "The Rise of the Stupid Network". *Computer Telephony,* August 1997, 16-26.

Jenkins, C. and B. Sherman. (1979). *The Collapse of Work.* London: Eyre Methuen, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Jhally, S. (1989). "The Political Economy of Culture", in *Cultural Politics in Contemporary America* (eds. Jhally and Angus, 1989) pp. 65-81.

Johnston, D., D. Johnston, and S. Handa. (1995). *Getting Canada Online: Understanding the Information Highway.* Toronto: Stoddart.

Kahn, H. (1970). *Forces of Change in the Final Third of the Twentieth Century.* Croton-on-Hudson, NY: Hudson Institute, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Lamberton, D.M., ed. (1974). *The Information Revolution. Annals of the American Academy of Political and Social Science*, vol. 412. Philadelphia: American Academy of Political and Social Science.

Large, P. (1980). *The Micro Revolution.* London: Fontana, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Large, P. (1984). *The Micro Revolution Revisited.* Totowa, NJ: Rowman and Allanheld, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Laurie, P. (1981). *The Micro Revolution: Living with Computers.* New York: Universe Books, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Lash, S. and J. Urry. (1994). *Economies of Sign and Space.* London: Sage.

Lessig, L. (1999). *Code and Other Laws of Cyberspace.* New York: Basic Books.

Lemley, M.A. and L. Lessig (2000). *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era.*

Lessig, L. (2002). *The Future of Ideas: The Fate of the Commons in a Connected World.* New York: Random House.

Lessig, L. (2002a). "The Architecture of Innovation". *Duke Law Journal*, 2002, 51, 1783.

Lewis, R. (1973). *The New Service Society*. London: Longman, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Lichthiem, G. (1963). *Europe and America: The Future of the Atlantic Community*. London: Thames and Hudson, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Machlup, F. (1962). *The Production and Distribution of Knowledge in the United States*. Princeton, NJ: Princeton University Press.

Mallet, S. (1963). *The New Working Class*. Nottingham: Spokesman Books, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Malhotra, Y. (1996). *The Theory of Coordination: A Critique*. Available at: http://www.kmbook.com/coordthy.htm.

Malone, T. W. (1997). "Is "Empowerment" just a Fad? Control, Decision-making, and Information Technology". *Sloan Management Review*, 1997, 38 (2), 23-35.

Mansell, R. (1993). *The New Telecommunications: A Political Economy of Network Evolution*. London: Sage.

Marcuse, H. (1991). *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*. (Originally published in 1964). Boston: Beacon Press.

Marris, R. (1964). *The Economic Theory of Managerial Capitalism*. New York: Free Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Martin, J. and A. Norman (1970). *The Computerized Society*. Englewood Cliffs, NJ: Prentice-Hall, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Martin, J. (1978). *The Wired Society: A Challenge for Tomorrow*. Englewood Cliffs, NJ: Prentice-Hall, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Martin, J. and D. Butler. (1981). *Viewdata and the Information Society*. Englewood Cliffs, NJ: Prentice-Hall, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Marx, G.T. (2001). "Technology and Social Control: The Search for the Illusive Silver Bullet". *International Encyclopedia of the Social and Behavioral Sciences*, 2001, 15506-15512.

Marx, G.T. (2002). "What's New About the New Surveillance?: Classifying for Change and Continuity". *Surveillance and Society*, 2002, 1(1), 9-29.

Marx, K. (1958). *Grundrisse, Outlines for a Critique of Political Economy.* Available at: http://www.marxists.org/archive/marx/works/1857/grundrisse.

Mathews, J. (1997). "Power Shift". *Foreign Affairs*, 76, 50-66.

McLuhan, M. (1964). *Understanding Media.* New York: Mentor, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Meynaud, J. (1968). *Technocracy*, trans. Paul Barnes. London: Faber and Faber, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Microsoft. (2001). A Platform for Web Services. Available at: http://msdn.microsoft.com/library/techart/websvcs_platform.htm.

Mosco, V. (1989). *The Pay-Per Society: Computers and Communication in the Information Age.* Toronto: Garamond Press.

Mosco, V. (1996). *The Political Economy of Communication: Rethinking and Renewal.* London: Sage.

Mulgan, G.J. (1991). *Communication and Control: Networks and the New Economies of Communication.* New York: Guilford Press.

National Research Council. (2002). *The Internet's Coming of Age.* Washington, DC: National Academy Press.

Nora, S. and A. Minc. (1978). *The Computerization of Society: A Report to the President of France.* Cambridge, MA: MIT Press, 1980, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Nortel Networks. (1999). *Policy Based Network Management.*

Nortel Networks. (2001). *2001 Annual Report.* Available at: http://www.nortel.com.

Nortel Networks. (2003). *Nortel Networks Introduces New Technologies to Deliver Enterprise Applications*. Available at: http://www.nortelnetworks.com/corporate/news/newsreleases/2003a/02_10_03_advanced_business_connectivity.html.

Odlyzko, A.M. (2003). *Internet Traffic Growth: Sources and Implications*. Available at: http://www.dtc.umn.edu/~odlyzko/doc/itcom.internet.growth.pdf

Olson, G.M., T.W. Malone and Smith, J. B. (2001), eds. *Coordination Theory and Collaboration Technology.* Mahwah, NJ: Erlbaum.

Online Computer Library Center. (2003). *Research Brief.* Available at: http://www.oclc.org.

Organisation for Economic Co-operation and Development (OECD). (2002). *ICT Investment in OECD Countries, 1980-2000.* Available at: http://www.oecd.org/dataoecd/45/20/2766404.xls.

Outsourcing Institute. (2001). *IT Index*. Available at: http://www.outsourcing.com.
Oxman, J. (1999). *The FCC and the Unregulation of the Internet*. Washington, DC: Federal Communications Commission, OPP Working Paper Number 31.

Pfeffer, J. and G.R. Salancik. (1978). *The External Control of Organizations: A Resource Dependence Perspective*. New York: Harper & Row.

Phillips, K. (1975). *Mediacracy: American Parties and Politics in the Communications Age*. Garden City, N.Y.: Doubleday, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Piore M. and C. Sabel (1984). *The Second Industrial Divide: Possibilities for Prosperity.* New York: Basic Books, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Pew Internet Project. (2005). *Broadband Adoption at Home in the United States.* Available at: http://www.pewinternet.org/pdfs/PIP_Broadband.TPRC_Sept05.pdf.

Porat, M.U. and M.R. Rubin, eds. (1977). *The Information Economy*. Washington, DC: U.S. Department of Commerce, Government Printing Office.

Postman, N. (1993). *Technopoly: The Surrender of Culture to Technology*. New York: Vintage Books.

Richta, R. (1967). *Civilization at the Crossroads: Social and Human Implications of the Scientific and Technological Revolution.* White Plains, NY: International Arts and Sciences Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Riseman, D. (1950). *The Lonely Crowd: A Study of the Changing American Character.* New Haven, CT: Yale University Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Robins, K and F. Webster. (1998). "Cybernetic Capitalism: Information, Technology, Everyday Life." in *The Political Economy of Information* (eds. Mosco and Wasko, 1998) pp. 44-75.

Roberts, L.G. (2002). *Internet Traffic Growth.* Caspian Networks.

Rostow, W.W. (1960). *The Stages of Economic Growth.* Cambridge: Cambridge University Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Saltzer, J.H. (1999). *"Open Access" is Just the Tip of the Iceberg.* Available at: http://mit.edu/Saltzer/www/publications/openaccess.html.

Saltzer, J., D. Reed and D. Clark. (1984). "End-to-end arguments in systems design". *ACM Trans. Comp. Sys.*, 2(4), 1984, 277-288.

Saltzer, J., D. Reed and D. Clark. (1998). "Commentaries on Active Networking and End-to-End Arguments". *IEEE Network*, 1998, 12(3), 66-71.

Christian Sandvig (2006). "Shaping Infrastructure and Innovation on the Internet". In *Shaping Science and Technology Policy: The Next Generation of Research* (eds. David H. Guston and Daniel Sarewitz). Madison, WI: University of Wisconsin Press.

Schiller, D. (1999). *Digital Capitalism: Networking the Global Market System.* Cambridge: MIT Press.

Schiller, H. (1969). *Mass Communications and American Empire.* New York: Augustus M. Kelley.

Schiller, H. (1973). *The Mind Managers.* Boston: Beacon Press.

Seidenberg, R. (1950). *Posthistoric Man: An Inquiry.* Chapel Hill: University of North Carolina Press, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Shaw Cable (2005). *Quality of Service Enhancement.* Available at: http://www.shaw.ca/en-ca/ProductsServices/Internet/ServiceEnhancement.htm

Smythe, D. (1981). *Dependency Road: Communications, Capitalism, Consciousness and Canada.* Norwood, NJ: Ablex.

Stadler, F. (1997). *The Nature of the Financial Networks.* Available at http://www.uni-muenster.de/PeaCon/eliten/financenet-stalder.htm.

Statistics Canada (2003). Information and Communication Technologies in Canada: A Statistical Profile of the ICT Sector. Available at: http://www.statcan.ca/english/freepub/56-506-XIE/56-506-XIE99000.pdf#search=%22information%20and%20communication%20technology%201995%207.6%20percent%20of%20Canada%20GDP%22.

Statistics Canada (2004). *Information and Communication Technologies: Contribution to the Economy.* Available at: http://www.statcan.ca/bsolc/english/bsolc?catno=88-003-X20040016799.

Stencil Group. (2001). *Defining Web Services.* Available at: http://www.stencialgroup.com/ideas_scope_200106wsdefined.html.

Stine, G.H. (1975). *The Third Industrial Revolution.* New York: G.P. Putnam's Sons, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Strassner, J. (2004). *Policy-Based Network Management : Solutions for the Next Generation.* Boston: Morgan Kaufmann Publishers.

Stonier, T. (1979). "The Third Industrial Revolution – Microprocessors and Robots." In *Microprocessors and Robots: Effects of Modern Technology on Workers.* Vienna: International Metalworkers' Federation, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Stiglitz, J.E. (1985). *Economics of Information and the Theory of Economic Development.* NBER Working Papers 1566. Cambridge, MA: National Bureau of Economic Research.

Summit Strategies. (2004). *Research Brief.* Available at: http://www.summitstrat.com.

Thompson, J.B. (1990). *Ideology and Modern Culture: Critical Social Theory in the Era of Mass Communication.* Stanford: Stanford University Press.

Toffler, A. (1971). *Future Shock.* New York: Bantam, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Toffler, A. (1980). *The Third Wave.* New York: William Morrow, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Tomeski, E.A. (1970). *The Computer Revolution: The Executive and the New Information Technology.* New York: Macmillan, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Touraine, A. (1995). *Critique of Modernity.* Cambridge: Blackwell, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

U.S. Department of Commerce. (1998). *The Emerging Digital Economy: Report on Electronic Commerce and Society.* Washington, DC.

U.S. Department of Treasury. (2000). *Report on International Economic and Exchange Rate Policies.* Washington, DC.

Vickers, G. (1970). *Freedom in a Rocking Boat: Changing Values in an Unstable Society.* London: Allen Lane, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Wellman, B. (2001). "Computer Networks as Social Networks". *Science*, 2001, 293, 2031-2034.

Winseck, D. (1997). *Reconvergence: A Political Economy of Telecommunications in Canada.* Cresskill, NJ: Hampton Press.

Winseck, D. (1999). *Illusions of Perfect Information and Fantasies of Control in the Information Society.* Paper presented to the Citizens at the Crossroads: Whose Information Society Conference, University of Western Ontario, London, Ontario, October 21-23, 1999.

Winseck, D. (2003). "Netscapes of Power: Convergence, Network Design, Walled Gardens and Other Strategies of Control in the Information Age" In *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.* (ed., David Lyon) New York: Routledge, 2003.

Whyte, W.H. (1956). *The Organization Man.* New York: Simon and Schuster, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Williams, F. (1982). *The Communications Revolution.* Beverly Hills, CA: Sage, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Wu, T. (2003). "Network Neutrality, Broadband Discrimination" *Journal of Telecommunications and High Technology Law, Vol. 2, p. 141.*

Wu, T. (2005). *Network Neturality FAQ.* Available at: http://www.timwu.org/network_neutrality.html.

Young, M. (1958). *The Rise of the Meritocracy: An Essay on Education and Equality.* London: Penguin, cited in Beniger, J.R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

ZDNet (2006). *AOL charged with blocking opponent's email.* Available at: http://news.zdnet.com/2100-9595_22-6061089.html.