INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI[®]

**CANADA AND THE INTERNET: THE CULTURAL
IMPACT OF AN
ELECTRONICALLY ENABLED CANADA**

By

Tamara Trudeau, B.A., hon.

A thesis submitted to the Faculty of
Graduate Studies and Research in partial fulfillment
of the requirements for the degree of
Master of Arts
in Canadian Studies

Carleton University

OTTAWA, Ontario

December 01, 2001

2001, Tamara Trudeau

**National Library
of Canada**

**Acquisitions and
Bibliographic Services**

**385 Wellington Street
Ottawa ON K1A 0N4
Canada**

**Bibliothèque nationale
du Canada**

**Acquisitions et
services bibliographiques**

**385, rue Wellington
Ottawa ON K1A 0N4
Canada**

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-72061-6

Canada

**The undersigned recommend to the Faculty of
Graduate Studies and Research acceptance of the thesis**

**“Canada and the Internet: The Cultural Impact of an
Electronically Enabled Canada”**

submitted by Tamara Trudeau, Hons. B.A.

in partial fulfillment of the requirements for

the degree of Master of Arts

.....
Thesis Supervisor

.....
**Acting Director
School of Canadian Studies**

Carleton University

Ottawa, Ontario

December, 2001

Abstract

This thesis will closely examine issues of intellectual property rights protection, personal privacy protection, technical, social and policy issues associated with the use of the Internet in Canada. It will explore some federal information technology initiatives and the role that the federal government and its regulators plan to adopt as the information-based economy becomes more established in Canada.

We conclude that it is doubtful that the federal government or any other public governing body would be able to establish a regulatory means for ensuring privacy to all members of the public. Instead, the future will be more likely to witness a transition from federal policy legislation, to private policy practice. This will be done through the use of code modifications, digital signatures, strong encryption practices, third party certification, intrusion detection, computer forensics, and reliable software.

Table of Contents

Introduction: Where We Came From – Charting The New Digital World	1
Introduction.....	1
Chapter 1: Internet Technology: The Medium	9
How are we connected to the Net?	9
T1 and T3 Traffic Carriage	11
Integrated Services Digital Network Data Link.....	12
Enter Asymmetric Digital Subscriber Line.....	14
The Cable Carriers: The Internet on Cable	15
A Wireless World	22
Chapter 2: Connecting Canadians: The Message? Content	27
The Big Attraction	27
Canada’s Self Discovery: The Internet Fosters Discussion and Democracy?	30
The “E”-Community	31
How Government is Helping	33
The “E”-Conomy	37
Personalizing the Electronic World	39
To Use the Internet or Not?	41
The Other Side of the Fence	45
Direct Democracy? No Thanks.....	46
Chapter 3: Connecting Government to Government: Strategies For Smarter Electronic Service Delivery.....	49
Government On-Line	49
Statistics Canada	51
Internet Use	51
Knowledge Economy.....	52
Dissemination Channels.....	53
Desktop Computing	54
Department of Foreign Affairs and International Trade	55
Electronic Service Delivery	58
Canada Customs and Revenue Agency	59
Security	61
ESD Design.....	62
ESD Strategy.....	63
Chapter 4: Technology Versus Technology: Battling The Demons Of The Electronic World With Policy And Code.....	66
The Great Beyond.....	66
Seducing the Powerless with Power	67
The Personal Information Protection and Electronic Documents Act.....	69
Technology versus Technology	73
Intellectual Property Rights and Privacy Protection Technologies	79
Encryption.....	79
Public Key Encryption.....	81
Digital Signatures.....	85
Password Protection.....	86

Intrusion Detection.....	87
Computer Forensics	88
Secure Wireless.....	90
Summary, Conclusions and Implications	93
Summary and Conclusions	93
Implications.....	98
Works Consulted.....	109

Table of Figures

Figure 1. Illustration of T1 traffic carriage	11
Figure 2. Twisted pair of ISDN service cables	13
Figure 3. Simultaneous use of Internet and television via Internet over cable services ...	17
Figure 4. Information traveling through various networks to arrive at receiving computer	18
Figure 5. CCRA's 3-tiered approach to electronic service delivery	63

Introduction: Where We Came From – Charting The New Digital World

Science Explores: Technology Executes: Man Conforms. (Lessig, 92)¹

Introduction

The Internet is not a phenomenon of the past ten years. The Internet is something that evolved from the social circumstances of the cold war and subsequently from decades of research, development and practical application. Its initial purpose was to ensure that in the event of a nuclear attack against the United States, the communications network between cities and bases would not be disabled. In the years following the end of the cold war, the Internet has become an international network of sub networks where users can experience a wealth of knowledge and entertainment.

The RAND GROUP first conceived of the Internet in 1964. The initial United States military network was comprised of four nodes – or computers – that were linked to each other in 1969 through a high-speed network. The network was designed to be anarchic, because in the event of a full-scale military attack on the United States, there would be no single way of disabling the information network that enabled military personnel to exchange strategic information. Consequently, access was limited to the military establishment.

The success of the system was based on a technology known as packet switching. Packet switching was designed to eliminate the need for specified routes of information

¹Lawrence Lessig. Code and Other Laws of Cyberspace. New York: Basic Books, 1999.

exchange (Abate, 7)². Messages would be divided haphazardly into packets and each packet would be wrapped in an Internet Protocol address. The address determined the final destination of the packet. Once the packet was sent into the network with its address on it, it could take any available direction to arrive at its final location, meanwhile switching from node to node. The order of the arrival of separately addressed packets from the same transmission would not matter as they would be re-ordered at the final destination and then opened, and read or viewed by the recipient. The successful implementation of packet switching guaranteed that the route that information traveled was unimportant given that information could successfully be bounced around the network until it reached its final destination even if communication points in between the sending and receiving sites had been destroyed. According to Bruce Sterling, if the “big pieces of the network had been blown away, that simply wouldn’t matter; the packets would still be airborne, lateralled wildly across the field by whatever nodes happened to survive” (Sterling, 1)³. The only thing that would matter was that the packet arrived, regardless of the route it took to its destination.

The success of the transfer of information from disparate sites was also largely attributed to the success of Network Control Protocol and later, by the higher-level technique known as Transmission Control Protocol / Internet Protocol (TCP/IP). Transmission Control Protocol converts messages “into streams of packets at the source, then reassembles them back into messages at the destination” (Sterling, 2). Internet Protocol “handles the addressing, seeing to it that packets are routed across multiple

² Janet Abate. The Pearly Gates of Cyberspace: a History of Space From Dante to the Internet. Cambridge: MIT Press, 1999.

³ Bruce Sterling. “A Short History of the Internet”. n.d. <www.eff.org/pub/Publications/Bruce_Sterling/FSF_columns/fsf.05>.

nodes and even across multiple networks with multiple standards” (Sterling, 2). The TCP/IP standard would not work with information that was not divided into packets. Consequently, packet switching was essential to the success of the TCP/IP standard and vice versa.

By 1971, there were fifteen nodes in the system, and it had become apparent that the computer-sharing nature of the network had been transformed into “a dedicated, high-speed, federally subsidized electronic post-office. The main traffic on ARPANET was ... news and personal messages” (Sterling, 2). The system that carried this data was known as the ARPANET because it was originally controlled and designed by researchers at the Pentagon’s Advanced Research Projects Agency (ARPA).

As the nature of Internet usage changed, access by computer into the ARPANET network was expanded to include universities and defense contractors (Carroll, p.43)⁴. The ARPANET was still in use until 1989; however, it was gradually replaced in the mid-1980’s by a new network, the National Science Foundation Network (NSFNet). Both ARPANET and NSFNet operated simultaneously until all users could be transferred to NSFNet.

While the NSFNet was evolving in the United States, in Canada “national research and academic networks provided a starting point for the establishment of a Canadian Internet Network” (Carroll, p.43). As a result NetNorth and CDNNet emerged. These two networks were not initially based on the Transmission Control Protocol/Internet Protocol (TCP/IP) standard established in the United States. They were, however, the foundation for the creation of the CA*net, which later adopted the

⁴ Carroll and Rick Broadhead. Canadian Internet Handbook: 1995 Edition. Scarborough: Prentice Hall, 1995.

TCP/IP standard. Once CA*net adopted TCP/IP, it was linked to NSFNet. This was an important step to replacing the more direct link to U.S. networks that some Canadian institutions already had in place (Carroll, p.43).

Linking existing networks to new networks began to emerge as a consistent pattern around the world. Finally, in 1991 the Internet was opened for public and consumer use by the National Science Foundation in the United States. This change predicated the arrival of Internet Service Providers in Canada and elsewhere, thus enabling market access to open, and thus allowing for the explosion of Internet services in the developed world (Lessig, 39).

In the years since, the Internet has become a site of human interaction. It has become a site where governments become transparent to their citizens and where businesses interact in an open forum. In Canada, the federal government has announced its mass integration of information technology and its growing transparency as an initiative to become more accountable to Canadians. The federal government's Government On-Line (GOL) initiative is designed to facilitate better government-to-citizen (G2C) and government-to-government (G2G) communication as well as Electronic Service Delivery (ESD). The Canadian government has determined that ESD is the electronic delivery of all existing G2C and G2G direct services. Electronic Service Delivery is also the electronic dissemination of sharable information resources. The nature of the Web, and the Intranets that are developed for use within governmental departments necessarily weaken barriers erected by the hegemonic structure of national government, as they open a communication forum on a high-speed, complementary channel that had not previously existed.

Before the widespread use of computers in the governmental and non-governmental workplace, ideas were housed within the confines of libraries and file rooms. Now, the information previously stored in warehouses is available to public servants and Canadian citizens alike through the use of efficient information management systems, high power electronic databanks and high-speed backbones, such as CA Net* 3, the third generation of the above-mentioned CA Net.

In the developed world, the Internet has experienced massive growth and as a result, has become a popular site for trend watchers and trendsetters. It has also become the site where our economy will likely experience the most new growth over the course of the next ten years. The Internet, however, is also fraught with ethical debates and issues of universalized connectivity, among others. High-speed Internet access has become a virtual necessity in the wake of unprecedented technological advancements that are bandwidth hungry. The federal government, federal regulators and private enterprises have attempted to tackle some of the issues related to high-speed Internet access and electronic service delivery over the course of the past ten years. Intellectual property rights protection and the trend towards convergence have prompted federal regulators to examine where Canada fits into the matrix of international connectivity. This thesis will closely examine issues of intellectual property rights protection, personal privacy protection, technical, social and policy issues. It will explore some federal information technology initiatives and the role that the federal government and its regulators plan to adopt as the information-based economy becomes more established in Canada. Resources from around the globe and, more specifically, from Canada have been assembled here and have helped to produce both questions and answers to some of the

issues that Canadians face as the Internet becomes a dominant force in our social, economic, political and personal lives. For this reason, the material presented herein is highly specific to the period in which the data was gathered and to the period in which the information was assembled for presentation.

The first chapter is intended to map out many of the popular technologies that currently enable computer-mediated communication and entertainment at the time of writing. While there is a brief overview of some emerging technologies, Chapter One is essentially conceived as a snapshot of the current state of the Internet, computer-mediated communication and the devices and tools that enable these things to affect change on our information gathering, communication and interaction patterns. Chapter One is a comprehensive overview of the tools most commonly used for computer-mediated communication. We pay specific attention to domestic Internet Services such as Asymmetrical Digital Subscriber Line and the Internet over Cable services.

The second chapter is intended to uncover and evaluate some of the reasons that Canadians are drawn to the Web. We explore how both the enabling technologies and the most sensitive issues tie together to form what is commonly referred to as the information economy. This chapter investigates both positive and negative aspects of widespread Internet usage. It projects some of the changes that are likely to be effected by the widespread use of computer-mediated information technologies.

The second chapter is intended to uncover and evaluate some of the reasons that Canadians are drawn to the Web. We explore how both the enabling technologies and the most sensitive issues tie together to form what is commonly referred to as the information economy. The second chapter looks at who is using the Internet and why.

We conclude that Canadians have great expectations of the Internet despite the insecurity associated with open-channel communications. We look at how the Internet is altering the communications landscape in Canada and we conclude that the changes effected are widespread and not necessarily wholly beneficial to Canada's social fabric.

The third Chapter looks closely at the Electronic Service Delivery strategies of three federal government departments; Statistics Canada, Department of Foreign Affairs and International Trade (DFAIT) and Canada Customs and Revenue Agency (CCRA). These departments were selected for their varied approaches to meeting the goals of Government-on-line as presented in the 1999 Speech From the Throne. The strategy that each department takes is evaluated against the peers in our review. We conclude that Statistics Canada is not likely to experience the level of success that both DFAIT and CCRA are expected to meet. We also conclude that DFAIT's goals are too lofty for current technology capabilities and current government funding levels. Additionally, we conclude that CCRA's ESD goals and history set it on the path to success. The biggest hindrance at this early stage will be the technology used to enable the level of security that Canadians demand from both the government and Internet-based transactions, and funding from Finance Canada.

The fourth Chapter investigates issues of privacy and intellectual property rights protection. It also introduces and evaluates some federal government policies designed to appease some serious citizen concerns. More specifically, we conduct an overview of Bill C-6, "The Personal Information and Electronic Documents Act". This Act is designed as an answer to some of the issues surrounding electronic publication as well as the sharing and collection of personal information over the Web. In relation to these

issues, a review of many of the technologies designed to counter document theft, and illegal reproduction of copyright protected information is also examined. We specifically address electronic encryption technologies, digital signatures, intrusion detection, computer forensics, password protection and the issues surrounding these methods as a means of anti-theft and anti-abuse protection.

Finally, the conclusion will bring together the issues that have been addressed throughout in an effort to illustrate that the Internet will bring about change to the Canadian public and most likely to the rest of the globe. These changes (positive or negative) will no doubt be met with criticism, skepticism, enthusiasm and doubt. We conclude that it is doubtful that the federal government or any other public governing body would be able to establish a regulatory means of ensuring privacy to all members of the public. Instead, the future will be more likely to witness a transition from federal policy legislation, to private policy practice. This will be done through the use of code modifications, digital signatures, strong encryption practices, third party certification, intrusion detection, computer forensics, and reliable software. The thesis will also offer judgment on some of the implications that the research raises. This thesis intends to uncover some of the issues that we are currently facing and some of the issues that we are most likely to face in the short-term future, as they relate to the Internet, Electronic Service Delivery, and the strategic management of information technologies.

Chapter 1: Internet Technology: The Medium

How are we connected to the Net?

When the Internet was first created, users were connected to the network at 1200 baud (1.2 kilobits per second) in *ideal* situations. This was done using a modem, which derives its name from its function. A modem is designed to modulate and demodulate bits of data from text to a computer-to-computer communications language. Modems were a necessary tool designed to transmit data over conventional phone lines by converting the electrical signal into a form that is acceptable for the Public Switched Telephone Network (PSTN). The reason for choosing a system which functions over the PSTN was that the infrastructure was already in place, allowing point-to-point communication with other existing devices. The PSTN carries high-frequency audio signals. In order for the transmission of data to be successful, modems were designed to operate over PSTN frequencies, producing binary data in a PSTN compatible form. Since computers communicate in binary format (10101010) signaling on and off operations, the transmission of a binary computer signal into an analog network signal is essential to the ability to transmit data across a network. As each access port to the network typically requires a simultaneous two-way capability, the transmission device must be able to perform both modulation and demodulation tasks at the same time, hence

the function of transmitting a digital signal into an analog signal is known as MODulation and the reverse is known as DEModulation: MODEM (Halsall, 57, 58)⁵.

In addition to the transmission delivery channels and hardware basics discussed below, it is also important to very briefly look at how data may be transmitted via these methods. Typically broadband mode is used for coaxial signal carriage. In Broadband mode, “available bandwidth is divided to derive a number of lower subchannels on one cable” as discussed during the T1 technology review below (Halsall, 49). Broadband mode is typically used as a concurrent transmission distribution technology, such as that delivered in a T1 or like fashion over the PSTN. As T1 and compatible technologies, cable and Digital Subscriber Line technologies leverage the existing communications architectures, they are the most common forms of high-speed Internet connections available at this time.

For at least twenty years, slow dial-up connections were the only method of connecting to the Internet; however, as technology evolved modem speed also evolved. Consumer modems became available in transfer rates of 14.4, 28.8, 33.6, and 56 kilobits per second (Kbps) during a period spanning 1989-1997. Dial-up connections are still among the most common means of connecting to the Internet for most residential users; however, high-speed technologies delivered at consumer prices are quickly overtaking the dial-up market in Canada and the United States.

In recent years networking technologies as well as connection speed have vastly improved. Users can connect in their work environments using T1 and T3 connections that allow them high-speed access to both their companies' Intranet and to the external

⁵ Fred Halsall. Data Communications, Computer Networks and Open Systems, Fourth Edition. United States: Addison-Wesley, 1995.

Internet. Users in a residential environment can also access high-speed connections.

High-speed Internet technology consists of at least three types of technologies: Integrated Services Digital Network (ISDN), Asymmetric Digital Subscriber Line (ADSL), and high-speed cable access.

T1 and T3 Traffic Carriage

T1 and T3 are high-speed digital networks that were designed by AT&T starting in 1957. Implementation of these networks began in the 1960's as a voice transmission network. The most significant change to the existing telephone system that T1 and T3 connections enabled was the digitization of the analog telephone system (Watchel, 1)⁶. A T1 line carries traffic at 1.544 Mega bits per second (Mbps); a T2 line carries traffic at 6.312 Mbps a T3 line carries traffic at 44.736 Mbps and T4 carries traffic at 274.176 Mbps. As the technology has advanced it has been matched by leaps in the speed at which it can transmit data. A T1 operates by splitting the existing line into voice channels, each equally divided into 64 Kbps. There are 24 of these channels on a T1 line and some extra bandwidth to perform synchronization of the lines.

Figure 1. Illustration of T1 traffic carriage

Typically when an organization claims that they are running T1, they mean different things:

They may mean that they have a network that is passing data at 1.544 Mbps; they may mean that they have a network that conforms to the T1 electrical interface

⁶ Bob Watchel. "All You Wanted to Know About T1 But Were Afraid to Ask". February 2001. <www.dcbnet.com/notes/9611t1.html>.

specification... or they may mean that they have a network that passes data that conforms to one of the several framing formats. (Watchel, 3)

For our purposes, we will be referring to a network that is passing data at 1.544 Mbps.

For voice traffic, a T1 carries analog traffic and converts it into digital traffic for carriage over the network and then returns it to analog status at the receiving end of the transmission. When a T1 carries digital traffic from sender to receiver, the conversion from analog to digital does not take place. This is where we see a difference in the standard use of modem technology. Most dial-up users connecting to the Internet are unable to connect directly to a T1 hub, thus requiring them to modulate data from its digital form to an analog form. In the case of the carriage of Internet traffic, the entire line is used to transmit data, which expedites transmission, as there is no unused portion of the T1 line at any time. For this reason, a T1 or like connection is extremely fast and efficient. Due to costs, however, a T1 electronic data connection is only available in the corporate marketplace.

Integrated Services Digital Network Data Link

Integrated Services Digital Network is a leased high-speed digital telephone service that can operate at five times analog modem service speeds. It is typically used in organizations that have a high rate of inter-site traffic volume (i.e. internal electronic traffic) (Halsall, 68). ISDN can transmit both voice and data without the use of a modem. This service converts the conventional phone line into a high-speed digital connection by dividing the existing copper cables into a three-channel system: there are two "B" channels and one "D" channel, as shown in figure 2.

Figure 2. Twisted pair of ISDN service cables

The B channels are used to transmit data at rates of up to 64 kilobits per second (Kbps), while the D channel performs administrative tasks that include establishing and dismantling calls and communicating with the telephone network at rates of 16 Kbps (Halsall, 464). Therefore, the line is typically established to carry 144 Kbps of data. Consequently transfer rates are very quick as data transmissions are established and dismantled by the system at rapid rates.

ISDN is used to carry both voice and data; hence the split line, which can carry both forms of traffic concurrently, or can allot both channels to data carriage. Unfortunately, due to the divided nature of the line, ISDN is highly sensitive to outside interference and noise, such as a bus driving by on a nearby road. While ISDN was one of the fastest connections available in 1998, faster services have since become available. As a result, ISDN technology has fallen out of favour, even in the workplace. It is still used in some environments; however, the cost of the service is prohibitively expensive.

Enter Asymmetric Digital Subscriber Line

Asymmetric Digital Subscriber Line (ADSL) is a technology that emerged in the mid-1990's as a copper line modem technology that promised to provide more bandwidth to residential subscribers (Knight, 103)⁷. A Digital Subscriber Line uses "the existing copper pairs in the telephone network to deliver more bandwidth than a regular phone line" (Knight, 103). It does so by capitalizing on unused frequency in the existing PSTN bandwidth. Earlier we stated that MODEM technology involved transferring digital information into analog information for transmission over the existing PSTN architecture in a form that matched the most commonly used frequency: that of voice. The original MODEM technology was only able to communicate over that limited high frequency, while ADSL transmission technology service splits the existing copper line into two different frequencies. This enables ADSL technology to capitalize on the lower frequencies that are unused during audio traffic communications. ADSL extends "the local loop to make it a true access network" that provides an always-on direct data connection (Knight, 103). Unlike the Internet-on-cable modem service (discussed below) ADSL access is not shared with other local users. It uses the existing local T1 connections to establish a direct data link between the user and the connection point (server). Consequently, ADSL can offer subscribers a dedicated twenty-four hour a day connection to the Internet at consumer prices.

Two key benefits of ADSL are dedicated bandwidth and choice of services (Knight, 103). This means that a dedicated quantity of the PSTN bandwidth is allocated for high-speed service that provides users with speeds of up to 960 Kbps downstream (to

⁷ Stefan Knight. "The Role of ADSL in Internet Access" Computer: July 1999, pp 9-10. Vol. 32, No. 7.

the home) and up to 120 Kbps upstream (from the home.) Additional services such as computer messaging and fax messaging to your personal computer are also available to ADSL subscribers; however at this time users cannot fax from their home computers using ADSL connections.

The Canadian Radio Television and Telecommunications Council (CRTC), the public body responsible for the governance of the *Canadian Broadcasting Act* and the *Canadian Telecommunications Act*, have mandated the opening of the High-Speed Internet market. Consequently, ADSL services that were originally only available through Bell Sympatico's High-Speed Edition are now also offered through some local ISP's. These services are provided through the existing PSTN architecture and, as such, are available at consumer prices because there are no infrastructure upgrades required. Typically the difference between Bell's High-Speed services and those offered by local ISP's is that a local ISP will often sell the subscriber the modem while Bell will not. Bell claims that they do not sell the modem to enable an upgrade to the system at any time without passing additional expenses along to the subscriber.

The Cable Carriers: The Internet on Cable

When the cable companies first announced that they would be offering Internet service over the cable line, consumers were not only surprised, but also confused. For years consumers had been duped by their own ignorance, believing that cable providers were only capable of offering a one-way service. The public was quickly proven wrong. Cable companies have been able to provide a consumer Internet service that theoretically exceeds the speed of ADSL. The Canadian Cable Industry (comprised of over 800 large and small federally licensed cable systems that deliver services to more than 7 million

Canadian homes) has responded to the increasing demands of high-speed Internet access in a number of ways.

As opposed to the conventional copper cable that the existing telephone structure uses, the cable companies have upgraded their system over the past decade from conventional copper cable to high-speed fibre-coaxial cabling. This combination of both fibre optics and conventional coaxial copper cabling will allow the cable companies to offer Canadians high-speed connections / services to the curb. Deployment of what is often termed “the last mile” technologies (i.e. fibre into the home) has yet to be implemented. At this time, the cost is prohibitively high for cable companies and the emergence of wireless technologies acts as an inhibitor to the expansion of the cable market as there is great risk involved in competing with more mobile and higher bandwidth technologies.

The service that the cable companies offer operates in a manner similar to ADSL. The bandwidth in the line is divided into frequencies. As only a prescribed portion is necessary to carry television signals, the remaining portion is ascribed for Internet service, thus allowing residents of the same household the opportunity to watch television and surf the Internet at the same time. In this respect, the service is similar to all other high-speed connections discussed thus far: the consumer can implement both the existing service and the high-speed connection simultaneously.

Figure 3. Simultaneous use of Internet and television via Internet over cable services

The cable industry has also adjusted the architecture of the existing system in order to rectify current weaknesses, such as net congestion and the downtime associated with pull technology. Net congestion is very similar to traffic congestion during rush hour. When there are more travelers on the road than the system can acceptably handle for the efficient transfer of vehicles from one location to another, traffic begins to slow down, back up and in many cases come to a halt. As a result, net congestion causes incomplete or painfully slow transmission of information across the network. In such instances, the user does not receive the full transmission, experiences timed-out or terminated transmissions, or experiences long delays because servers and network components are being used beyond their capacity or are overloaded. Net congestion in audio applications is typically accompanied by a gap in the reception, which can irritate users and prompt them to seek audio service where the network components are better equipped for heavy traffic.

Pull technology occurs when a user visits a web site and essentially pulls bits of information from a selected site, “across various networks involved in the transmission, through to the users local Internet Service Provider (ISP) and ultimately to the end user’s computer via a local access network” (The Internet and Beyond 2.1)⁸.

Figure 4. Information traveling through various networks to arrive at receiving computer

Regardless of geographic location, every other user accessing the same information will also have to pull the “same bits across the Internet – possibly using the same regional or backbone network repeatedly to carry precisely the same information thousands of miles” (The Internet and Beyond, 2.1). Since the network is designed to take the fastest route to the end-user’s systems, it is not uncommon to see a pattern of transmission that in no way reflects a logical route to the naked eye. In the event that the user is seeking bandwidth-hungry data, information is more slowly received (i.e. net congestion.) Where real-time information is being downloaded (such as live video,) there is usually jitter in the

⁸ The Internet and Beyond: Canadian Cable Industry. Canadian Cable Industry. March <www.ccta.com>.

reception, which is caused by changing network delays. The reduction of the use of pull technology, designed to eliminate or reduce these problems, is a high priority for all Internet service providers. The cable industry's answer to this problem is to place frequently accessed information closer to the user. They do this by creating what they call a parallel Internet. This practice is carried out in two ways: the first involves creating a more efficient link to sites that are more commonly visited and the second involves placing frequently accessed information closer to the user. The purpose of placing the information closer to the user – a practice that is known as caching – reduces the distance that information must travel. For example, if neighbor A goes to the Microsoft website and downloads an update for Windows XP Office Suite, and then neighbor B requests the same update, that information will be pulled across the network for both users twice over a more conventional connection. Caching eliminates the need to pull that information twice. Instead, the information is pulled through the cable companies' high-speed backbone, or head-end (connection point) and through to the local network. It is cached at the backbone in the event that users in the same local network might also like to access the same information. In some cases, cached information is continually updated at the head-end, thus saving the user from ever having to pull the information its full distance. The cable companies only cache information that is frequently accessed.

The next phase of the Cable Industry's connectivity initiative addresses the issue of *connectivity*. Cable providers have already begun deploying digital set-top boxes to some regions. The boxes are capable of converting conventional analog television sets into multimedia terminals. As about 99% of Canadian homes have one or more

television sets, capitalizing on this medium will bring the Internet to users who might not otherwise be able to afford it or are unfamiliar with current computer technologies (The Internet and Beyond, 2.3). The set-top box acts as both a port to the Internet and the hard-drive needed to operate the television, keyboard and mouse in a computer-like fashion. As these tools are more likely to be in the financially-acceptable range of many new users (the cost of a new computer can typically cost between \$1800 and \$3000) the likelihood of the set-top box deployment to be a successful short-term impetus to becoming knowledgeable about the Web is very high.

The cable industry's final connectivity initiative is the development of enhanced services for use over high-speed networks (The Internet and Beyond, 3.0). This will include the addition of videoconferencing and IP Telephony (real-time voice transmission over the Internet) to its current information systems. Videotron of Quebec, a cable company that has been acquired by communications giant Quebecor, has been testing IP Telephony over its high-speed networks. Some drawbacks to this technology at this time are low transmission speeds, voice delay and the appearance of audio gaps due to lost or severely delayed packets. Packets that arrive out of order are discarded when using real-time applications; hence blank spots or silences appear in the transmission. For this reason, there is an obvious flaw in the use of TCP/IP packet switching for bandwidth hungry real-time information exchanges. This is an issue that is currently under review by many telecommunications organizations, research groups, university programs and independent hobbyists.

Canadian businesses and universities have been quick to recognize the communication possibilities that high-speed Internet connectivity can provide. Given

that the majority of users today are still connected to the Internet via dial-up lines, DSL and cable modem connections will become more popular as user needs increase.

Furthermore, as technologies advance at a rate of approximately a 6-9 month upgrade release cycles, the need for more bandwidth increases, as newer applications are typically more complex and more bandwidth-hungry. Higher speed technologies will enable services such as Voice over Internet Protocol (VoIP), videoconferencing and real-time document sharing to users who have the requisite hardware and software.

High-speed Internet services have not been perfected by any means. Although the speeds at which ADSL services are offered to customers are moderately lower than the theoretical maximums available via cable modem, some tests have shown that in many cases “higher sustained download speeds could be obtained by” Sympatico’s High Speed Edition (Bell, 32)⁹. This is in part due to the fact that the Sympatico service is offered in a closed loop service (explained earlier), which guarantees that the user does not have to share the line with other nearby users. The shared nature of the cable companies’ deployment of Internet service provision has sparked much competition and debate between ADSL’s dedicated services and the theoretically shared line offered by the cable providers. Rogers claims that its service is offered at a rate of 3 Mbps upstream and downstream; however, “the shared bandwidth nature of the cable technology coupled with the fact that” a “cable modem can only go as fast as the speed of the sending site,” will continue to limit top-end speed (Bell, 32). Furthermore, the theoretical maximum offered by the cable companies assumes that the user is not operating a television somewhere else in the home at the same time. Rogers has also experienced difficulties

⁹ Mark Bell. “Connectivity: Broadband rules!” Monitor. March 2000 pp. 32-34. Vol7. No. 8.

with its email servers. This difficulty often means that subscribers do not receive email messages for long periods at a time. To date, this shortcoming has yet to be permanently resolved.

A Wireless World

Wireless technologies are also experiencing strong growth as they are more easily deployed, upgraded and serviced with the added bonus that they offer higher bandwidth than coaxial and fibre technologies. The most obvious demand upon wireless technologies in Canada and elsewhere is that they be ready to operate anytime and anywhere. This type of flexibility is essential to the success of a technology as we become more mobile as workers, students, children, parents and citizens. Indeed, the flexibility associated with wireless technologies is likely the larger impetus for its widespread implementation and its subsequent success.

Wireless technologies deploy a different system of telecommunications than wired technologies. Wireless technologies use radio frequencies to deliver their service, while wired technologies use the term “frequency” in a different fashion. For use in the wired world, frequency refers to the rate at which a signal can be reproduced, and the channel capacity to ensure that a signal will experience minimal or zero signal deterioration. Therefore, we can see that the meaning of the two words in both markets signals a different understanding of the transmission of data traffic.

Transmission over radio frequencies is necessarily accompanied with a different set of deployment restrictions than that which we would see over wired systems. For instance, current results show that there is an increased risk of transmission interference from physical obstructions (hills, mountains, buildings.) However, there is also promise

of creating a high-speed wireless connection that is capable of circumventing transmission obstructions. Wireless services that already exist include, cellular voice service, wireless two-way email, Web browsing and more. The term “cellular,” which is the one we most often see, “derives its name from the way geographic areas are broken into small cells, each with its own transmitter/receiver and antenna” (Skvarla, 2)¹⁰. The cells range in size from 2-20 miles in diameter. They communicate with a users’ cellular device and with a centrally located switching station, which then connects with the regular landline telephone system. As a wireless user moves from one cell to another, the central switching station switches the user to a new cell and a new frequency. To most users, the frequency is irrelevant regardless of the device they are operating – 850 MHz for cellular phone or 1800MHz for Personal Communications Devices (Skvarla, 2). In remote areas, wireless technologies are the best option because coaxial or fibre bandwidth is offered at a premium if it is available at all.

Gartner analyst, Carol Skvarla writes: “the use of wireless technologies mainly focuses on providing a wireless extension to the main wired network services” (Skvarla, 3). This is in part due to the facts that wireless technologies are not widely implemented for data communications at this time and because the PSTN architecture is already heavily burdened with supporting the Internet infrastructure.

Until recently, the wireless tools allowed users to receive but not send data over the wireless network. As the expansion and growing popularity of the wireless market demands increased services and two-way communication, we are now witnessing a transition in the options of wireless services. There are currently four major technologies

¹⁰ Carol Skvarla. “Wireless Technologies and Services: Overview”. United States: Gartner, Inc., 2001.

ving for the wireless Internet market: cellular phone services, private packet radio technology, satellite services, and spread spectrum technologies. Many wireless Internet services are based on one or more of these services. As cellular phone service is currently the leading architecture for wireless systems in many regions – Canada among them – it is expected that citizens who currently have Web-capable phones will have increased services from their providers as phones and other personal digital devices begin to offer services that operate seamlessly over the cellular system.

In accordance with this assumption, many software companies have been developing platforms and applications for use on wireless devices. Ottawa's Accelio, formerly Jetform, has released an application that allows users to view forms and spreadsheets over wireless Internet. Benefits of wireless technologies not only include mobility of services, but also lower prices for greater bandwidth, the wireless substitution of wireline services, and the bundling of wireline and wireless services.

According to Gartner, Inc., however, companies that currently offer applications over the wired Web are not producing applications that fit users' needs and, consequently will not succeed. Significant changes will have to be made to current services in order to provide users with the impetus and flexibility that they demand of a wireless device. In addition to the improvement of wireless services, personalization of services will also become a success factor: "Successful mobile applications and services are those that focus on personalized, location- and time-relevant information and services" (King, et. al., 2)¹¹. In this regard, in a bandwidth-limited environment, the ability to personalize service will increase effectiveness and add value to the service.

¹¹ Michael King, Delia MacMillan, Adam Sarner, Alexander Linden. "Wireless Web Data Services: Personalize or Perish". United States: Gartner, Inc., 2001.

To conclude our discussion on wireless and wireline data communication technologies, it is important to note that there are security risks associated with the implementation of all of these technologies. Security risks tend to be augmented with wireless devices because that transmission takes place exclusively over radio frequencies, which are more easily decrypted than their wireline counterpart frequencies. This issue will be further examined in Chapter 4.

In addition to current and forthcoming high-speed Internet connections, users must also have the requisite hardware to connect to the Internet. Wireline users will need a computer with at least a Pentium, or other like class hard drive for IBM compatible systems, at least 12 megabytes of Random Access Memory (RAM), at least 20 Megabytes of free hard disk space, a video card, and a copy of Windows 3.1, or greater, or almost any recent edition of the Unix Operating System, or another compatible operating system. Aside from the hardware, the operating system software enables users to process high-speed data transmissions and view advanced graphics while at the same time expediting communications. The above-mentioned hardware and software products are the most basic components required for Internet connectivity. They will deliver the user a very slow connection. As Internet services grow, and as commercial-level hardware and software platforms become more advanced, the success of the above-mentioned devices dwindles and will eventually become incompatible with all current and forthcoming services available over the Internet. Users wishing to access the Internet through high-speed connections will require much more advanced hardware including more RAM, a more advanced operating system, a more advanced video card (for viewing

graphically rich web pages, services and forms) and a higher-bandwidth Internet connection.

As we can see, keeping up with the pace of technology can be extremely challenging if not, next to impossible for most. In addition to the complications associated with learning and integrating a new technology into our lifestyles or business operations, there are also the costs associated with these tools and services. The impact of Internet technologies is being felt across our culture, in ways that we could not have predicted even ten years ago. We turn our discussion now to the impact that Internet technologies have had and will continue to have on Canadian culture.

Chapter 2: Connecting Canadians: The Message? Content

The Big Attraction

“Moore’s Law states that the performance of silicon microchips doubles every 18 months” at no extra cost to the consumer (Taylor, 277)¹². Faster processors are being created at unprecedented intervals “for enthusiasts who want state-of-the-art performance and features for the Internet, as well as advanced applications such as video editing, digital imaging, and 3-D gaming” (Macedonia, 124)¹³. As was evident in Chapter 1, high-performance computers and chips are designed to perform high-speed tasks. At this time in history, we are witnessing the creation of advanced hardware and information services that may become commonplace in no time at all, just as accessing the Internet has become commonplace for many Canadians.

Over the course of the past 3-5 years, the nature of Internet usage has changed dramatically. We have witnessed a revolution from a tool that allows contact and file transfer, to a tool that allows business to be conducted around the globe at the click of a button. All of these innovations beg the questions: what did people go there for in the first place? What was it that made the Internet so attractive? The answer is simpler than might be expected: people came to the Internet for *each other*.

¹² J. Taylor. “Engineering in the Information Age”. Engineering Management Journal. December 1998. pp. 277-287. Vol. 8 No. 6.

¹³ Michael Macedonia. “Why Digital Entertainment Drives the Need for Speed”. Computer Magazine. February 2000. pp. 124-127.

In the beginning, people reached each other through research groups and chat rooms. In its early days, the Internet was a place where people could talk to each other without constraint, without judgment and without prejudice. Social markers of race, colour, gender, hearing, sight or other physically noticeable or socially limiting disabilities, became invisible in light of the medium, in light of the purpose. Today, the Internet is thriving largely because, aside from being tracked through the use of cookies, users are allotted an anonymity that real space must create (Lessig, 33). Many users feel that they benefit from being able to move from one site to another without having to share details about themselves. Users enjoy the freedom that assuming a new identity can pose. They enjoy the fact that when they enter into cyberspace, they can leave all of their personal problems between the chair and the keyboard and become something different for a short while.

The ability to create an alternate self also presents a serious issue in relation to protecting innocent victims from harmful strangers who purport to be someone they are not. It is this characteristic, however, that attracts many users to the Internet. It is also this characteristic into which many marketing agencies are eager to tap. They are eager to create profiles of consumers who access vendors of popular Internet-marketed goods such as books, compact discs, dvd movies, computer games and other entertainment goods and services. Marketing profiles are created because of the aforementioned lack of visual markers associated with in-person purchasing. For vendors, knowing who their clients are is of paramount importance if they are to expand their business. Chapters.ca for instance, used the Chapter1 card and the email addresses of consumers to market new books, goods and services to its known clientele. This allowed the company to sell new

products and services through the direct knowledge of a customer's purchasing history as computer-mediated purchasing makes recommendations based on live interactions with storefront personnel impossible.

While the Internet's growing popularity has inspired governments and corporations to communicate and market differently than they have in the past, the knowledge exchange that popularized the Internet more than two decades ago is still an overwhelmingly important factor of its success. In this respect, the Internet is empowering because it invites participation and sharing (Levine, Locke, Searls, Weinberger, 17)¹⁴. Canadians have also been coming to the Internet to share, participate and become part of the national community. Canadians are looking for a better understanding of who we are and how we fit in. We are looking for a valuable site in which we can participate, instead of observe. Instead of fragmenting and creating chaos, the Internet can have the power to be a medium for sharing. The Internet can help us understand who we are by the stories we share and by the commonalities that we encounter on a daily basis.

There are many ways to look at what's drawing us to the Web: access to information, connection to other people, entrance to communities, the ability to broadcast ideas.... They all come back to the promise of voice and thus of authentic self. (Weinberger, 43)

The Internet has the ability to allow us to show our true selves while at the same time, keeping secrets or creating an alternate self - the self we would like to be. As we have just learned, the power to unite people is a contributing factor to the success of the Internet in Canada.

¹⁴ Rick Levine, Christopher Locke, Doc Searls, David Weinberger. The Cluetrain Manifesto. Cambridge: Perseus Books, 2000.

Canada's Self Discovery: The Internet Fosters Discussion and Democracy?

Canada's size has enabled the development of an advanced communications network, but never before have we used it so efficiently. Never before have we used our telecommunications network for more than the exchange of business and family matters. The Internet enables the communication of self. It enables Canadians to share how they feel about where they live, to link that with how others feel about where they live, and thus to place themselves within a matrix of members of a larger, and somewhat disparate community of communities.

David Weinberger, author and philosophy instructor, writes that there is

nothing more intimately part of who we are than our voice.
It expresses what we think and feel. It is an amalgam of the
voluntary and involuntary. It gives style and shape to
content. It subtends the most public and the most private.
It is what we withhold at the moments of greatest
significance. (42)

The sharing of voice can be a place of important self-discovery. Over the past year, for instance, the largest new Internet user increase was among teenage girls. According to a study released by Jupiter Communications and Media Metrix, the teenage girls demographic has grown five times faster than the Internet overall (Klotz)¹⁵. Teens are heading home from school and web chatting with their friends for long periods of time. They are extending the social atmosphere of the school into their homes.

Furthermore, teenage girls are not only using email, or chat like their Internet communication predecessors; they are using instant messaging and ICQ (I seek you) communications. According to Dr. Arlette Lefebvre, a psychiatrist at Toronto's Hospital for Sick Children, the reason for the success of real-time conversations is that youth who

¹⁵ Hattie Klotz. "Teen Girls Stage Their Own Web Revolution". Ottawa Citizen: Tuesday August 22, 2000 <www.ottawacitizen.com>.

might otherwise be shy or embarrassed to talk about something personal are freed with the removal of facial cues (Klotz). We return here to the fact that the removal of social barriers fosters a type of discussion that is not easily facilitated in person-to-person contact. The removal of personality or physical traits that inhibit us in our daily lives frees us to discuss subjects (often of an intimate or personal nature) that would make us uncomfortable in person. This can be an important communication factor for awkward teenagers. The introduction of the always-on high-speed connection has also allowed teens to log on in record numbers. With this tool, they can communicate instantly without tying-up family phone lines - an important link in the teenage social circle.

The “E”-Community

As a result of the Internet and the connectivity it enables, many Canadians can look to each other for knowledge, cultural growth, business enhancement and a better understanding of their country and its government. The web is the site where all of these things converge to create a new economy and a more accountable business and governmental model. It is also the home of virtual communities and to a growing extent, the home of local communities meeting in a virtual atmosphere. The Internet is not by any means a Utopia, but rather an additional and complimentary communications channel.

The Internet’s success is currently heavily based on market constraints: popularity of a web site or chat room is equal to advertisement and financial gain; acceptable norms are equal to popularity. Acceptable norms meet one or more of the following criteria: the ability to meet the privacy demands of the general public; the reputation of a company that has practiced business in a brick and mortar store front, the collection and proper use

of personal information; and / or the adherence to laws concerning the collection and use of personal information and the maintenance of a secure site that promises that the privacy of individuals is kept from hackers, thieves and criminals. There must be acceptable norms to achieve popularity, to retain consumers, and to make a profit. Without these characteristics, there is considerable constraint placed on the success of an Internet site, chat room, or the Internet as an entity.

The World Wide Web is a global environment whose structured chaos is daunting to many potential new users. To ease some of the trepidation that these people might have, Andrew L. Shapiro, author and legal scholar, suggests that we construct “*high-quality, web-based* local community networks that are ubiquitous, accessible, and interesting enough so that all Net users will want to use them” (Shapiro, 213, author’s emphasis)¹⁶. Local community networks would have to be designed to appeal to users of all ages. If created, such a network would offer users a free, local gateway or portal to community Web sites and to the larger Internet. The advantage of the gateway would be to bring together users for reasons of both common interest and geographical proximity.

To a limited extent, the Internet has adjusted how we encounter people and make new friends or acquaintances. If we could establish a free local gateway to the Internet, then users from designated local areas would be able to use that portal to meet people in their region and share stories of local interest. They would also be able to attain information and news about their community along with a list of upcoming events. Shapiro notes that the portal system would “ensure a degree of involvement with community issues and engagement with actual neighbors... we would do better to think of them as local gateways to the global Net - and to offline interaction as well” (213). It

¹⁶ Andrew L. Shapiro. The Control Revolution. New York: Public Affairs, 1999.

is the sense of community that can be created by sharing the virtual life in the physical realm that has the potential to unite members of local communities. The establishment of free local gateways would also help the federal government work towards some larger goals: 1) the establishment of universal access; and 2) the enhancement of localism. A burgeoning example of a gateway with the potential discussed above would be www.OttawaStart.com. The site is fairly holistic in its approach; however, at this time it is missing the strong tie to government, free web access and chat areas that a free local gateway would offer to residents of a geographical community.

How Government is Helping

The establishment of local gateways (discussed above) is a logical extension to the federal governments' attempts to become more transparent and accountable to Canadians. It would also compliment many of the initiatives established by the *Connecting Canadians* agenda. The purpose of *Connecting Canadians* was to foster participation in global connectivity. It was also designed to help move Canadians into a leadership role in the global knowledge-based economy and to further the national goal of becoming the most connected country in the world by the year 2004. Industry Canada has created the *Connecting Canadians* initiative in response to growing trends on the Internet and as an opportunity to expand both our global and domestic new media markets. The initiative offers five different programs to foster the use of the Internet and its resources to rural and urban Canadians of differing financial backgrounds. The mandate of the *Connecting Canadians* initiative is to "help Canadians become the most connected people on earth, ready for the jobs and opportunities of today's knowledge-

based economy” (*Connecting Canadians*, 2000-17E)¹⁷. Industry Canada also offers a *Connecting Canadians* information kit to interested parties. There are five major programs that fall under the *Connecting Canadians* umbrella.

The first of the five programs is called “Connected to Government.” This site and service offers Canadians an access point “through which Internet users around the world can obtain information about Canada, its government and its services” (*Connecting Canadians*, 2000-17E). The site offers a link to all online governmental departments, its employees, federal initiatives, task forces, programs and services as well as provincial and municipal governments and programs. It is a federal channel designed to help establish a more accountable government through the sharing of knowledge, federal public documents, Acts of Parliament and other issues of public interest, for Canadians and global citizens alike.

The second service offered is called “Connected to Business.” The Connected to Business’ *Strategis* program offers research materials regarding business information and trade data along with hundreds of links to business-related sites around the world. The service also offers tips to small businesses. The second “Connected to Business” program is the “Student Connection Program” (SCP). This service provides small and medium-size businesses with customized training that ranges “from ‘getting connected’ and using E-mail to advanced search techniques, Internet banking” and E-Commerce. The third and final “Connected to Business” program is called “ExportSource.” This service provides business users with “current trade information, export preparation, trade show preparation and international project bids” (*Connecting Canadians*, 2000-17E).

¹⁷ Government of Canada. Industry Canada. Connecting Canadians Information Kit. Ottawa: 2000.

The Department of Foreign Affairs and International Trade (DFAIT) has an important role to play in the “ExportSource” program.

Industry Canada’s third *Connecting Canadians* initiative, “Connected to Youth,” is comprised of three smaller programs. The first, “SchoolNet,” offers users more than one thousand learning services and resources (*Connecting Canadians*, 1999-8E). Its mission is to encourage the integration of information technology into the classroom and to make sure that students obtain the learning and research skills that they will need to function proficiently in Canada’s information-based economy (*Connecting Canadians*, 1999-8E). The second program, “Campus Worklink: National Graduate Registry” (NGR) offers senior secondary and post-secondary students access to new job opportunities (*Connecting Canadians*, 2000-17E). “Canada’s Digital Collections” provides youth with multimedia work experience while at the same time making Canadian content accessible on the Internet through the digitization of text, images, and audio/visual material.

The fourth *Connecting Canadians* program is called “Connected to Consumers.” This program offers a wide range of consumer oriented tips on subjects that range from auto leasing, bank fees, health and safety issues (*Connecting Canadians*, 2000-17E).

The fifth and largest project is called “Connected to Communities.” This program encompasses five smaller programs. “Smart Communities” involves making the most of opportunities that new technologies can offer, such as better health care delivery, better education and better training. This is done through community demonstrations. “CanConnect” is a motivational initiative to encourage all citizens to help prepare Canada’s young people for the challenges of the next century. This program is carried

out on-line through the showcasing of various opportunities at schools and community sites across the country.

Perhaps the two most important programs carried out by the *Connecting Canadians* initiative are the “Community Access Program” and the “Computers for Schools Program.” The “Community Access Program” aimed to connect 5000 rural and remote communities to the Internet before March 31, 2001. This program aims to bring new opportunities, new skills and more knowledge to all Canadians, regardless of their geographical location. The “Computers for Schools Program” aims to provide schools and libraries with refurbished computers and software donated by both the public and private sectors. This will provide greater access through volunteerism and donation practices, as opposed to hefty federal and private sector financial investments (*Connecting Canadians*, 2000-17E). Through these two programs, a local gateway system could be established, offering Canadians of all financial backgrounds free access to issues that are timely and community-relevant. A server at municipal headquarters in all participating regions could run the local gateways, thus enabling a national program, devoted to local content. The “Community Access Program” and the “Computers for Schools” programs both offer Canadians the opportunity to take a leadership role in their local communities and on the global Internet. Extending these programs to offer community gateways will only enhance the experience of the Web for users on local and global bases.

The final program, “VolNet,” offers computer equipment and Internet connectivity to approximately 10 000 voluntary organizations across the country.

Consequently, the Canadian government has adopted a plan to foster growth in Canada's growing technology-driven market.

The *Connecting Canadians* project, which is funded in part by Industry Canada, municipal governments and corporations aims to give Canadians the tools they need to get connected to the Internet and start contributing to the information-based economy. Moreover, it also gives Canadians the opportunity to connect to each other, to share their community experiences and to create a sense of belonging within both the local and national communities by inviting participation by all.

The "E"-Conomy

According to a 1999 Statistics Canada evaluation, e-commerce comprises all transactions carried out over computer-mediated networks. Under this definition, *Interac* transactions are also included as they are carried out over computer-mediated networks. In Statistics Canada's most recent survey of e-commerce transactions, however, *Interac* transactions were excluded for the purpose of measuring Internet transactions only, which are typically carried out over *open-platform* computer-mediated networks. Fostering market growth through the widespread use of Internet business tools marks a major shift in the use of the Internet. What started out as a communications tool and information network has been transformed into a model for conducting business. In July of 2000, Statistics Canada revealed that one in ten companies used the Internet to sell goods in the 1999 calendar year. This number amounted to 0.2 per cent of their total economic activity (*The Daily*)¹⁸. Considering the adoption rate of the Internet in the market place, a 0.2 per cent share of revenue is quite impressive, accounting for 4.4 billion dollars of

¹⁸ Government of Canada. Statistics Canada. E-commerce and business use of the Internet The Daily, Ottawa: August 10, 2000. <www.statcan.gc.ca>

retail revenue in 1999 alone. It is anticipated that the Canadian market share of Internet commerce will increase substantially over the next five years to 93.67 billion, or 5 per cent of the world share of Internet commerce activity (*The Daily*). These numbers testify to the high corporate adoption rate of the Internet and to the Government of Canada's efforts to continue along the path of making Canada the most connected country in the world (*Throne Speech*, 1999)¹⁹. Ensuring that Internet commerce flourishes as the economy shifts from a resource-based economy to a knowledge-based economy is part of the federal governments' plan to assume a leading role in the new global economy. There are various ways that the government has fostered growth in this sector of the economy. As we have already seen, the *Connecting Canadians* agenda accounts for a major component of ensuring strong market growth. Recognizing that the knowledge market is constantly evolving, the federal government has also initiated other steps to ensure that Canada remains abreast of technological change.

High powered computing devices and connection services expedite electronic business (e-business) and electronic commerce (e-commerce). E-Business and e-commerce are the foundations of the information-based economy. The Government of Canada defines electronic business as "activities carried over computer-mediated channels" (*Reality Check*, 8)²⁰. From this definition, they have defined electronic commerce as "transactions carried over computer-mediated channels that comprise the transfer of ownership or the entitlement to use tangible or intangible assets" (*Reality Check*, 8). Thus defined, e-commerce is a sector within e-business. E-commerce is

¹⁹ Government of Canada. Parliament. Speech From the Throne. Ottawa: 1999. <www.parl.gc.ca>

²⁰ Government of Canada. Statistics Canada. A Reality Check to Defining eCommerce. Ottawa: 1999.

perceived to be a channel that will compliment existing commerce channels, while at the same time expanding market visibility and consumer choice (*Reality Check*, 9).

E-commerce, just as with conventional commerce, is associated with the exchange of goods from one party to another. Typically, there are two electronic transactions that take place when a consumer commits to purchasing goods or services over the Internet. The first is a commitment for goods or services and the second is a commitment for payment (*Reality Check*, 15). In order for the success of e-commerce to be measurable, there must be a means of determining a point at which a transaction occurs. Consequently, Canada's federal government has determined that a transaction has occurred when two parties commit to an "explicit or tacit contract" for the exchange of goods or services, i.e., when one party agrees to purchase the goods and / or services of another party (*Reality Check*, 15). As long as the transaction is carried out over electronic channels, it is considered to be an e-commerce transaction. If, however, a consumer browses the Web and then calls an order number phone line, or goes to the site of business to make the final purchase, then the transaction is not an electronic one.

Personalizing the Electronic World

In addition to adopting the Internet as a twenty-four hour a day shopping environment, users are also interested in the ability to personalize their daily experiences of the world through Internet media and computer software tools. The ability to personalize the media you receive and the way you view your desktop is a feature that appeals to many users. Services that focus on the users preferences such as "My Web," "My Documents," "My Computer" are marketing tools that dupe users into believing that they have control over what they see and read. Users are duped because they are fooled

into believing that the convenience of adding or removing operative parameters offers them the opportunity to have complete control and access to that which they choose, but how much choice does a user have when presented with limited and strictly defined options? Users can only adjust settings on their desktops within the parameters established by the software they use. Personalization is a popular trend with Web and computer services. It is easy to forget that it is a tool exercised by producers to fool users into believing that they have as much choice and personal control as they could imagine.

In addition to the personalization trend, users are witnessing a growing number of sites / information services they can search with their search engines, yet engines such as Yahoo! and Canada.com have stated that they have only logged about one tenth of the information available on the Web. While authors like Rick Levine, Christopher Locke, Doc Searls, and David Weinberger point to the benefits of the freedom of choice and personalization that the Internet has brought to users others, like Mark Kingwell, point out that this new freedom comes at a cost:

We have been given, in place of meaningful individual liberty and the freedom of escaping social bonds, merely the freedom of unimpeded information flow. What kind of freedom is this? The freedom to be overwhelmed? The freedom to be afflicted by the clamouring voices of a million other users? If genuine freedom means greater control over one's life, a greater ability to direct oneself and make choices, then the freedom offered on the Internet is hollow indeed. 145²¹

Kingwell's commentary alerts us to the power the Internet has. The freedom to access information of all types can be a hindrance to novice users. What his discussion does not focus on is the power to teach that the Internet can bring to users. Through

²¹ Mark Kingwell. Dreams of Millenium. Toronto: Penguin, 1999.

personalization and customized searches, users have instant access to information that may have previously taken them months to track down. The speed at which a person can find the information that they are seeking through the use of the Internet is not to be easily dismissed. While personalization tools are limited by the code that commands how much personalization is capable, they also allow for a certain degree of choice and a wide range of information access options. Yet it cannot be stressed enough that in the realm of personalization, choice is limited both by the amount of options and the quality of information delivered. Given that most users will look at a maximum of the first one hundred hits when they conduct a search, the key will be to make searching easier and more efficient in an effort to deliver more precise information resources. There is no doubt that there is a world of information and commerce services available to us, but will we continue to look for them, or will we settle with what is most easily available to us? This author believes that most users will select the most convenient and relevant options, regardless of their pecking order.

To Use the Internet or Not?

When radio was first introduced into the consumer market, it was “touted as an opportunity to provide more education and public service programming” (Macedonia, 124). When computers were first introduced into the consumer market, they were marketed in a similar manner, offering users the opportunity to help in household financial and organizational tasks, while at the same time providing a learning tool to youngsters. History, however, has revealed more popular uses. The success of radio can best be attributed to its ability to bring entertainment to the masses at low costs. The rapid growth of computer technologies for the home market has followed a path similar

to that of radio. According to Michael Macedonia, “Entertainment - defined as amusement, recreation, or diversion - cuts a swath through human experience wide enough to include computing” (125). Thus, the entertainment industry, which includes all forms of media, has a pivotal role to play in computing innovation and the growth of the computing market over the course of the twentieth and twenty-first centuries (Macedonia, 126).

Oftentimes, the urge to be entertained can take perverse directions such as accessing online pornographic services. While the immense penetration of pornography is not a particularly endearing feature of the Internet for many, we can neither ignore its presence, nor the fact that many users view it as entertainment. In addition to pornographic media, interactive gaming is also extremely popular. Most games require the latest high-speed computing technologies just to run. Others require a high-speed Internet connection - in addition to a high-power computer - so that users can navigate their way through games in groups, or so that they can battle each other in real-time. The creation and widespread use of interactive media have prompted technology producers and equipment manufactures to design faster, better components and games so that users will continue to purchase hardware and software to run better, faster, more interactive tools and games. The design and creation of high-performance computers and high-speed Internet access technologies are symbiotic markets that are driven by their ability to entertain users at the click of a button. We can conclude, therefore, that the *need for speed* is driven largely by the demand for more interactive and realistic forms of online entertainment, as much as it is by the yet-to-be created bandwidth-hungry applications,

faster and more secure open-channel transactions and more responsive information exchanges desired by government and corporations.

At the time this document was researched, approximately 13 per cent of Canadian homes, 52.8 per cent of Canadian businesses and 95.4 per cent of the Canadian Public sector are connected to the Internet, and those numbers grow exponentially annually (*The Internet and Beyond*, 2.3 & *Review of StatCan Survey*)²². In July of 2000, The Public Interest Advocacy Centre published a report outlining which groups of Canadians use the Internet and which do not. The study concluded that non-users were *not* comprised of one homogenous group. Those who are connected to the Internet are largely members of middle to high-income families. Those who are not connected to the Internet were noticeably divided into two groups:

the first group is near-users, those who have varying degrees of interest in being connected, but are unable due to a number of barriers, of which the most important are cost/affordability and literacy. The second group, distant-users, consists of people who have little or no interest in the Internet and online services, or perceive no value in the Internet to meet their everyday economic or social needs. (Reddick, 9)²³

Therefore, there are currently two very different groups of Canadians that do not access the Web. Members who belong to the first group of non-users tend to have the desire to use it and tend to perceive the value of becoming connected; however restrictions of various natures prevent them from doing so. For this group of users, they are most likely to connect to the Internet through libraries, Internet cafés and community education programs. They are the most likely group to educate themselves on the values and

²² Government of Canada. Statistics Canada. Review of Statistics Canada Survey. July, 2000
<www.statcan.gc.ca>.

²³ Andrew Reddick, Christian Boucher and Manon Groseilliers. The Dual Digital Divide. Ottawa: The Public Interest Advocacy Centre, 2000.

services of the Internet. The greatest challenge that members of this group are likely to face is accessibility to publicly funded Internet services. Some questions arise: If they are close to public facilities, can they find the time to get to the services and learn how to use them? If they are living in rural communities, will they find transportation of their own to get to the facilities where free services are offered? These questions are not easily answered. In fact, the questions cover a much larger issue than Internet connection - they instigate questions relating to the accessibility of all services for Canadians living in economically depressed situations.

Of those who comprise the second divide, the study suggests that they face “technical and cost-barriers” along with a certain complacency towards the necessity of the services and educating themselves on how to use the Internet (Reddick, 3). Improving content, design and anticipating user needs is expected to increase access among this group of non-users. The study shows that there is a non-exclusive tendency for members of the second divide to be in their pre-retirement or retirement years (45 + years of age). Further, the proportion of women is slightly higher in this group than the proportion of men, so it becomes increasingly necessary to offer services that respond to the needs of women in this age group. Of particular and growing interest to the women in this group are health care services. These services (there are many) provide the 45+ female cohort with the impetus to access the Web, as there are services that speak to their personal needs. Reaching members of the dual digital divide through the removal of accessibility barriers and through the creation of more responsive and intuitive on-line services will dramatically increase the perceived value of Internet services and thus, the concentration of Internet users in Canada. At this time, it is impossible to determine if

this hypothesis will retain validity or not. As these are the main barriers listed by Canadians who are not currently accessing Internet services, it is highly likely that the removal of inhibitors will increase usage, and thus perceived personal value.

The Other Side of the Fence

In addition to reasons of economic ability or lack of perceived need cited for not connecting to the Internet, there are others who have logged off of the Internet for various reasons. Mark Kingwell argues that much of the conversation of Internet chat rooms and newsgroups has become banal and trite:

Mostly the newsgroups merely remain in the realm of the banal. You can find ones devoted to everything from Lisa Simpson's college of choice to foot fetishes, alien abduction tales, and Jean-Luc Picard's sexual tastes. (Kingwell, 147)

Author and scholar Mark Kingwell notes that perhaps the greatest reason for the change in the quality of information exchanges over the Internet was the advent of widespread accessibility brought about by the opening of the Internet market in 1993. In addition to the growing banality of Internet chat and content, the unfortunate infusion of electronic crime, pornography, hate propaganda and other offensive content have also taken a strong hold of the Internet. Addressing pornography and hate propaganda is proving as difficult as addressing electronic crimes.

While there are many who would agree that the creation of commercial services like America OnLine and others that helped to connect every willing and capable person to every other willing and capable person was a good thing, there are others who would disagree. This open connection not only fostered the vast communication and information sharing discussed above, but it also brought about what Kingwell calls Prole

drift: users could no longer be certain that “another user was a university student, let alone another professor or high-tech worker” and this change is what Kingwell, Kroker, and Weinstein²⁴ call the dumbing down of the Internet communications forum (Kingwell, 149).

Direct Democracy? No Thanks...

Despite all of the benefits associated with more open communication among teens and other members of Canadian society, we cannot help but recognize the fact that the immense access to information brought about by the widespread introduction of the Internet is fostering a world of false hopes and unattainable dreams. For example, the creation of truly democratic governance discussed in some newsgroups would actually help to remove the hard-won rights of many social groups that struggle for recognition from the margin:

The technophile's dream of direct democracy is actually undemocratic: it threatens the freedom of the few by appearing to accede to the interests of the many. Centralization of power, while often dangerous, is necessary if we want to protect threatened minorities... It is also necessary for accountability... Direct democracy will be functionally invisible. Decisions that affect us will be made by sheer force of numbers. True, we can use our own terminals to protest a decision, but when the protest ends, so does our freedom. There will be no capitals to march to then, no legislatures to picket. (Kingwell, 152)

Kingwell's discussion makes it plain that the Internet, while powerful and beneficial to society on many levels, will not automatically transform Canadian or global society. It will not cure our social ills. It will not bring about a new governance model and it will not create the semblance of a Canadian national identity. It will not solve crimes nor cure

²⁴ Arthur Kroker, Michael A. Weinstein. Data Trash. Montreal: New World Perspectives, 1994.

diseases, although it may *eventually* contribute to remedying all of those things. In the form it appears to us today, the Internet is complimentary to all other existing communications channels, and thankfully so. It is dispiriting to imagine a world where voices are drowned out by the power of the masses. The voices of the few are equally important as the voices of the many; and while all voices may not have the power to positively change society, it is important that a forum for the delivery of their social and political positions continues to exist.

We have established that the Internet has taken on a life of its own over the course of the past ten years through the directions of entertainment and commerce, pornography and crime, e-business and banal chatter. We have established that Canadians and the federal government have high expectations of the Internet. Providing more and more Canadians with access to high-speed connections should enhance the growth of the technology-based market place and it should theoretically help Canada compete with other countries as we change from a resource-dependent economy to an information-based economy. For this reason, the Canadian Radio Television and Telecommunications Council (CRTC) has officially decided not to try to regulate the Internet in Canada. It has done so citing the importance of focusing on research and development as well as information technology education in an effort to drive the information-based economy. For this reason, the government of Canada encourages further hardware, software, and connectivity creations by granting research and development organizations tax breaks. The federal government has also enabled the growth of the communications market, by deregulating telecommunications providers, opening up the local and long-distance telephone market, and innovating at its National

Research Council Laboratories. Fostering telecommunications partnerships also positions federal representatives favourably as it illustrates foresight and their ability to react to the changing technology landscape in which their constituents carry out their daily lives. In chapters three and four, we will investigate what some federal departments are doing to make electronic service delivery (both internally and externally) a reality for the Canadian public and how regulation of the electronic channel will evolve in the months and years to come. More specifically, in the next chapter, we will take a look at the strategies that three federal departments are implementing to tackle the issues that are posed by performing old tasks with new tools, and new tasks with new tools over the electronic channel. We will compare the effectiveness of each strategy and determine which of the three departments is taking the best path to success.

Chapter 3: Connecting Government to Government: Strategies For Smarter Electronic Service Delivery

Government On-Line

The 1999 Speech from the Throne mandated that Canada would become the most connected country in the world by 2004. The Treasury Board of Canada Secretariat (TBS), the federal organization responsible for the distribution and requesting of Parliamentary funds for large projects undertaken in all governmental departments, has been placed in charge of the Government of Canada's Government-On-Line (GOL) initiative. Treasury Board Secretariat is responsible (among others) for allocating funds to major information technology, information management and GOL initiatives within all federal departments. This section will investigate the role that information management and information technology plays in three federal departments and their Electronic Service Delivery initiatives on the following two levels: Government-to-Government (G2G) and Government-to-Citizen (G2C). In doing so, we will examine some of the internal efforts that have been implemented or planned by the selected departments to bring more efficient electronic service delivery to all concerned parties. This section will look closely at some of the initiatives that have been leveraged by Statistics Canada, the Department of Foreign Affairs and International Trade (DFAIT), and Canada Customs and Revenue Agency (CCRA). Statistics Canada has been selected because it is the single greatest repository of information in the country, holding private, personal, corporate and national data of both sensitive and non-sensitive natures. The Department of Foreign Affairs and International Trade and Canada Customs and Revenue Agency

have been selected because they are among the four most powerful departments in the country. Known as Super-Ministries, these two play an integral role in service delivery to Canadian citizens located around the globe²⁵.

The ability to deliver services electronically while at the same time effectively managing information internally is essential to all Canadians. Furthermore, issues discussed throughout this study (information technologies that enable service delivery on a worldwide scale, privacy rights protection and the reasons why citizens are choosing electronic service delivery) all play an important role in why all government departments, and for the purpose of this discussion, these departments, are adding electronic service delivery to the list of current service delivery channels. The intention of electronic service delivery is to offer more choice to Canadians and of course, to eventually offer it as a replacement to the paper-laden delivery of Government-to-Citizen services.

To enhance G2C service delivery, the government has also recognized that most Canadians do not draw borders between departments. Furthermore, many federally undertaken initiatives cut a swath across many different departments. Given this knowledge, the government has undertaken an initiative to have several departments host “clusters” of information. These clusters will act as portals to various departments, agencies, non-government organizations and private sector companies that play a part in various government programs or mandates. Each of the departments we will investigate have launched their funding requests to participate in any number of the approximately 30 clusters that the “O Canada” site will play host to through the 3 Gateways: Canadians, Canadian Businesses, and non-Canadians.

²⁵ The two other super-ministries are National Defence and Human Resources Development Canada.

Statistics Canada

According to chief statistician Dr. Ivan Fellegi, “Statistics Canada is well on its way to meeting the GOL requirements as far as... dissemination and communication services are concerned” (@Statcan, 23)²⁶. In early 2001, Statistics Canada released a review that outlined their progress in all information service delivery initiatives. The document, titled @Statcan, investigates what directions the department is taking to achieve the GOL mandate set out by the Speech from the Throne in 1999. Specifically, the department has taken initiatives to study and release new data on Internet use and identify what comprises the knowledge-based economy. In addition to these initiatives for information released to public, Statistics Canada has also made improvements in the realm of Government-to-employee, Government-to-Government and Government-to-Citizen service delivery through improved desktop computing and dissemination channels.

Internet Use

Without data on the penetration and adoption of Internet use by Canadians, the GOL initiative could be prepared for certain failure. Statistics Canada believes that

Information on household use of the Internet is an important indicator of Canadian families’ readiness to benefit from Internet services; that is, their readiness to use the Internet to acquire information, to take advantage of distance learning, *to use government online services*, and to participate in e-commerce. (@Statcan, 17) (emphasis added)

For this and other reasons, Statistics Canada conducted a survey in 1999, the results of which were released in May of 2000. The study indicated that household use of Internet

²⁶ Government of Canada. Statistics Canada. @Statcan: Special Issue 2001. Ottawa: 2001.

services increased year-over-year from 36% to 42%. The study also revealed that Internet use in the home is now more prevalent than in the workplace or at schools. The study also noted “virtually all public sector institutions ... used the Internet” (@Statcan 17). These indicators help keep the government-wide initiative of Government online on track because they support the assumption that Canadians want and will use electronic service delivery through Internet channels.

Knowledge Economy

Statistics Canada completed and published a study in 2000 that asked where the ‘old economy’ ends and where the ‘new economy’ begins. While new technology firms are portrayed in the public as the arbiters of the new economy, the study showed that public views on what comprised the new economy were incomplete and that the “new economy may actually be much larger and more widespread” than had been previously thought (@Statcan, 21). The study also found that industries that did well using some measures of high-tech didn’t necessarily perform well in all qualifying categories. The study did conclude however, that at this time, most industries and businesses are combinations of both old and new economy business models. Ultimately, the study concluded that at this time, there are no indicators of the new economy that apply to all industries and business models, which necessarily makes the definition of what comprises the new economy an elusive one. While several other agencies, private sector businesses, education centers and research facilities all have definitions of what comprises the new economy, the federal government through Statistics Canada has concluded that it is simply too soon to determine the exact sources and indicators of what comprises the new economy.

Dissemination Channels

Statistics Canada runs an internal dissemination channel (Intranet) called CANSIM II. The purpose of CANSIM II is to act as a communications and information dissemination tool to all employees of Statistics Canada. CANSIM II will eventually deliver a “comprehensive electronic database of all publishable statistics” (@Statcan, 22). The purpose of this Intranet stretches beyond a more efficient means of delivering resources to members of the Statistics Canada community; it also serves to meet the goals set out in the *Personal Information Protection and Electronic Documents Act* (discussed below). The Act notes that all information that the government previously made available on paper must now be made available electronically. In fact, there is much debate over whether it would be best to move to an entirely electronic model internally or not. Such a transition would help reduce the nearly four hundred percent increase in paper usage in government since the distribution of the Internet to the desktop began in the early 1990’s.

In addition to the internal dissemination channel, Statistics Canada has made changes to its external web site mapping to the “common look and feel” of all governmental web sites to increase usage of the service. The changes have been an overwhelming success. Usage of www.Statcan.ca increased by fifty per cent in just one year. The actions that were taken to improve the site include:

- Market research regarding the reasons for visits and overall satisfaction with the results of visits;
- Increase in number of resources for students;
- The addition of more electronic copies of traditional publications;
- A reengineered version of the monthly Retail Trade publication;
- The reorganization and inclusion of abstracts of all Research Papers on the site;
- The addition of timely information for public reception (such as the addition of Federal Electoral District Profiles days after the calling of the federal election)

These changes, along with changes made to the “O Canada” website and several others helped enhance the Internal and external delivery of information to Statistics Canada Employees and Canadians alike.

Desktop Computing

In order to ensure the effective delivery of all services, it is essential that Statistics Canada run its desktop computing systems efficiently. To maintain a path of continual growth, Statistics Canada plans to upgrade its desktop operating system to Windows 2000 over the course of the year 2001. This transition will be followed “by a move towards standardization of office automation software” in the fiscal year of 2002-2003. In addition to these changes, the refreshing of hardware technologies as they become obsolete will also take place. These changes to the desktop will also enhance the departments’ plan to develop a capacity for electronic data collection. These changes are especially important, as many of Statistics Canada’s corporate clients have requested the transition because it is easier for them to communicate electronically with the department. Once the adoption of electronic reporting has been incorporated, a significant proportion of respondents will be ready to take advantage of this option allowing them to transfer numbers from their systems directly into Statistics Canada’s.

While Statistics Canada has taken a public approach to their delivery and fulfillment of the GOL initiative, there are, of course, shortcomings. First, we see that the automation of back-office systems – back-office automation is associated with data processing, inventory, and accounting – has come as an afterthought (Menzies, 60)²⁷.

The systems that support electronic service delivery should have been in place and in use

²⁷ Heather Menzies. Whose Brave New World? Toronto: Between the Lines, 1996.

before www.Statcan.ca became a tool for public use. Furthermore, the automation of electronic information collection should already be in place internally to ensure the effective delivery of the systems before they are released to the public. Statistics Canada's approach to GOL / ESD suggests that there is far too much emphasis placed on the government's necessity to deliver services over the Internet. Historically, government has been a slow adopter of technology. Now, however, they are expected to deliver services in an environment where they are simply unprepared to operate at the level of efficiency that the public expects. Either steps must be taken to ensure due diligence has been followed and internal operations are more efficiently managed from both technology and human capital aspects, or else the programs will be destined for failure and / or intense public scrutiny and backlash.

Department of Foreign Affairs and International Trade

The Department of Foreign Affairs and International Trade has taken a very different approach to electronic service delivery than has Statistics Canada. DFAIT has started the process by recognizing the internal strengths and weaknesses of their organization. First, they have placed emphasis on the fact that their employees are their greatest strength. Furthermore, they have also recognized that these employees are essentially knowledge workers and "good information management and information technology (IM/IT) makes them more effective, and enables them to innovate and adapt their programs to the changing needs of Canadians" (*DFAIT Plan*, 1)²⁸. The advent of the mass implementation of information technologies in the workplace of DFAIT has not been without its complications. Changing from an organization that operated solely on

²⁸ Government of Canada. Department of Foreign Affairs and International Trade. DFAIT Information Management Strategic Plan. Ottawa: July, 1999.

paper to one that operates with electronic messaging has instigated the perception that consistent record keeping has vanished with the paper on which it was printed.

According to DFAIT's IM/IT plan, this feeling of lost records is leading to a belief that the organization is losing its corporate memory. In an effort to preserve this "memory," employees are regularly filing electronic transactions on paper, thus wasting paper.

Furthermore, if their employees' record management was more consistent, the records would be placed on a community server where all members of a work community within DFAIT would be able to access the information.

Second, DFAIT made an attempt to develop an information management strategy. The first step with this plan was to develop an understanding of what was meant by the expression "information management strategy". They have concluded that the goal of a strategy is to "match changing business directions with changing IM/IT: to chart, in a constantly changing environment, a direction which identifies the best total solution for the business needs" of Foreign Affairs (*DFAIT Plan*, 1). The plan identifies five needs that are common to all of DFAIT's lines of business. The framework outlined in the Information Management Strategy is designed to be carried out over several years and to map back to larger federal initiatives. Hence for DFAIT the entire framework for delivering electronic services over Internet channels lies in establishing sound internal practices and then moving them to the public realm.

Foreign Affairs has established a single department-wide computing architecture that is enforced through the use of common hardware and software environments. The establishment of enforced internal standards was essential to the deployment of the three

worldwide internal electronic channels that DFAIT uses for communication to its 130 worldwide offices.

Given its role in monitoring and maintaining import and export laws, regulations and transactions (with the help of Canada Customs and Revenue Agency), DFAIT must run over 70 applications on its internal systems to ensure the sound operation of the programs and to ensure minimal downtime given that the businesses it runs must operate continuously.

DFAIT firmly believes that they must adopt sound practices of internal e-commerce before they can bring their operations to the public. They have implemented a plan to do so by

- Integrating departmental directories;
- Enabling electronic authentication and authorization for the acquisition of goods and services;
- Developing an application architecture for ESD;
- Aligning their business with Government-wide initiatives for Service to the public and;
- Building a data warehouse.

These steps, while they may seem logical and simple, are massive undertakings for an organization with the size and scope of DFAIT.

Perhaps the single greatest challenge that an organization such as DFAIT faces is security concerns. How do they ensure safe and secure transactions over public channels? In their own terms, DFAIT believes that no one system can offer “both complete assurance of security and all of the functionality that its users require” (*DFAIT Plan*, 18). Given this, there is overwhelming attention focused on both securing the information transacted while at the same time making it easily facilitated. As a federal department DFAIT is required to adhere to government-wide security policies over the

Internet and for all electronically generated transactions. As such, DFAIT will begin using the federal secure channel once it has been implemented. They will also be using Entrust security software for Public Key Infrastructure (PKI,) the issuance of digital signatures and certificate authentication for all electronically generated transactions. In addition, DFAIT is required to adhere to the regulations set out in the *PIPED Act*, explained in Chapter 3.

Electronic Service Delivery

DFAIT believes that electronic service delivery not only saves paper and time, but it also streamlines processes and ensures procedure adherence. To reduce paper related processing, the Department is moving towards an “electronic transaction-processing model for high-volume manual transactions” (*DFAIT Plan*, 22). This process requires that the Department re-engineer its processes to reduce transactions, and to provide a more efficient approach to processing them. The use of electronic signatures instead of manual signatures expedites the processing of internal forms such as leave forms. The Department believes that by enabling internal service delivery through practices such as electronically filing for leave, DFAIT can be assured that their programs function well internally. They can then take their internal lessons and move them to the sphere of public electronic service delivery.

It is believed that the Electronic Service Delivery Strategy will

- Enable Electronic Authorization and Authentication;
- Align with Government-wide initiatives for Service to the Public; and
- Establish a data warehouse (*DFAIT Plan*, 23)

These, along with other initiatives, are expected to set DFAIT on the path to achieving government-wide goals as well as efficient Government-to-Business and Government-to-Citizen service delivery.

We can see that DFAIT has a much more comprehensive approach to the delivery of electronic services to the public than that of Statistics Canada. DFAIT's approach, which is much more focused on the efficiencies of its back-office systems, is more holistic and likely to be more successful than Statistics Canada's approach. The single greatest reason for the likelihood of the success of DFAIT's electronic service delivery strategy lies with the fact that streamlining back-office systems expedites external service delivery through the efficient management of information needed to process claims, requests and services. Conversely, the all-encompassing approach that DFAIT has taken to enable electronic service delivery may be a hindrance to the success of the program because government funds are limited and the scope of the program is likely to exceed funding arrangements through Finance Canada and the Treasury Board Secretariat. Furthermore, programs such as DFAIT's, that have a completion life exceeding one year tend to have reduced success rates as funding for all government departments and programs is issued on a year-to-year basis from April to March, matching the federal government's fiscal year.

Canada Customs and Revenue Agency

Canada Customs and Revenue Agency (CCRA) is perhaps the only federal department that has been in the business of electronic service delivery before there was a term for it. The Customs portion of the department has a history of producing customs transactions electronically for large corporations such as auto parts and automobile

manufactures. They have historically done this through the advance notification and authentication of shipments of goods, the certification of delivery agents and the verification of goods received with the manufacturer. This process proved so efficient that the Department moved towards delivering other services through electronic channels. They added telefile for the telephonic filing of income tax claims. This entire process was conducted using a data warehouse system that recognized callers by their social insurance numbers and processed claims accordingly.

CCRA has long been at the fore of the implementation of high technology for the purpose of streamlining processes. When the 1999 Speech from the Throne announced that Canada's government would be the most connected government in the world by the year 2004, CCRA took steps to "become a model user of information technology and the Internet" (*Strategy for ESD*, 1)²⁹. The Department began the careful task of integrating many of their highly sensitive operations into online service delivery channels.

Periodically, the Department sets out new goals in an effort to meet the promise of the 1999 Speech from the Throne. After the Year 2000 crisis had been averted and the Department could turn its attention to new projects, a new strategy was developed. The strategy, published in March of 2000, set out Goals, created a vision and used guiding principles to manage the goals. The full integration of Electronic Service Delivery was designed to:

- Make it easier and more convenient for businesses and individuals to claim credits, as well as to file, report, and remit duties and taxes;
- Simplify the registration of businesses;
- Streamline the reporting and clearance of people and goods through customs; and
- Serve as a catalyst for Canadians to adopt electronic commerce.

²⁹ Government of Canada. Canada Customs and Revenue Agency. Strategy for Electronic Service Delivery. Ottawa: n.d.

These goals were designed to make the delivery of services much easier for CCRA. In the process and not unintentionally, CCRA became a champion of electronic service delivery as the department that directly touches the lives of more Canadians than any other federal department³⁰.

The ESD strategy that CCRA has been implementing is designed to eventually offer Canadians, Canadian businesses, and Canadians living outside of Canada the ability to select from an assortment of “secure, automated, self-service channels to their tax and customs obligations” (*Strategy for ESD*, 2). The holistic approach to G2C services at CCRA will eventually allow for the packaging of services designed to meet the needs of particular client communities and will be accessible through the “O Canada” web site. The services will be customizable, based on citizen needs and will be focused on understanding what those needs are.

Security

The need to offer Canadians secure services over the Internet is perhaps more important at CCRA than at any other department. The nature of the information held and processed by CCRA is of an extremely sensitive nature as it exposes many details about an individual that cannot be gleaned without full disclosure from the individual. The possibility of the personal information of Canadians falling into criminal hands is a very serious concern for CCRA officials. In keeping with the solemn promise to retain all information private and confidential, CCRA takes very strong security measures when processing any transaction, especially electronic transactions over “open” channels such as the Internet. In fulfilling its mandate to retain all information private and confidential,

³⁰ CCRA touches the lives of approximately 22 million Canadians each year.

CCRA has built itself the reputation of being the most trusted institution in the country (*Strategy for ESD*, 4). While at the same time promising the safety and security of personal information, the Department recognizes the breach of this confidentiality as a possibility and as a risk that they must bear.

ESD Design

To enable ESD, CCRA must have a clear design strategy that will meet all of its targets of enabling full access services via the Web and soundly ensure the protection of all shared information. The vision of the design is based on the successful integration of the current print-version services into the electronic channel and with the effective marrying of service delivery with other governmental agencies. In an effort to facilitate this process, CCRA will design services so as to:

- Give clients access to all their records in an integrated and intuitive fashion (learn about your employment history through HRDC; learn about your taxation history through CCRA, etc.)
- Design services to be independent of the delivery channels being employed (all services offered can be delivered via all delivery channels)
- Facilitate use by clients with special needs (web services will be enabled to function for the visually impaired, or the mobility impaired)
- Build in the flexibility to facilitate the changing needs of clients, CCRA's changing role, and technical innovations (as technology and needs change, the system will be flexible enough to change accordingly)

The security, adaptability and functionality of CCRA's web services will be essential to the success of the Electronic Service Delivery Strategy. If for some reason, cost extends beyond the Department's budgets for implementation, key factors in the design could be compromised and the end result could be significantly off the mark of the vision they have set out. Given the early stage of electronic service delivery over open channels, the

outcome of visions as lofty and idealistic as CCRA's becomes a reality, as technologies are developed to map to the vast needs of such complex organizations.

ESD Strategy

Approximately ten years ago, CCRA began on its path towards electronic service delivery with their Getting Government Online agenda. The approach has since been revised and now includes a three-tiered implementation plan to take place over a five-year period. The plan outlines an evolutionary process from one-way transaction processing to a fully integrated approach offered through various levels of government (federal, provincial, municipal.)

Figure 5. CCRA's 3-tiered approach to electronic service delivery

The first tier, "Online presence", is already enabled. The second tier, "Fully enabled", is partially functioning at this stage. The partial enabling of the second tier has allowed

citizens to “e-file” their taxes and to monitor the progress of their tax claims. The integration of wireless technologies and services delivered through mass-access devices such as television will expand the possibilities of the second tier service offering. The use of PKI technologies, to be explored in Chapter 3, is heavily leveraged in this stage. The third tier, “Seamless government”, is a few years in the distance, but its intent is clear because most Canadians do not draw borders between governmental departments. The creation of seamless government through the electronic channel eliminates those borders for citizens, thus allowing for seamless service delivery across departments, and levels of government whose responsibilities are of varying natures.

CCRA believes that to successfully implement electronic service delivery they will have to overcome the barriers and risks associated with the technologies used. As we have seen with Statistics Canada and Department of Foreign Affairs and International Trade, they are not alone in this struggle. All government departments, including those at the provincial and municipal levels, (which were not explored in this examination,) must overcome the barriers associated with electronic service delivery if the goal of becoming the most connected country in the world is to be realized by 2004. Beyond the obvious uses of information technologies, it is unknown why there is such a race to be first in full service integration. There are clear and measurable shortcomings associated with being first in the realm of technology implementations.

Organizations that are first to adopt new technologies often have to contend with the bugs of new software programs. They are also often faced with limited choices, uncontrollable expenses and backlash from the teams that are required to use the tools on a daily basis to perform their jobs. Furthermore, there is also a significant increase in the

likelihood of failure. The expected success and integration rates are high among Canadian citizens, yet resources and acquisition and integration procedures considerably restrain the ability of the government to pursue projects at the velocity expected by constituencies. It is therefore debatable whether or not the success of any of the three far-reaching government departments reviewed in this section will be able to successfully follow through on the strategies they have laid out for the years to come. We now turn to a detailed discussion of the direction that information technology security will take over the course of the months and years to come.

Chapter 4: Technology Versus Technology: Battling The Demons Of The Electronic World With Policy And Code

The Great Beyond

High-speed computing technologies are increasingly more imposing on the Canadian cultural landscape. As we cannot stop the force of this Goliath, we must learn to cope with the changes that these high-speed computing technologies bring. How we cope with these changes shapes the outcome they affect on our daily lives. Integrating technology into our daily lives not only eases transition from one technology to another; it also enhances our transaction and communication channels. In Canada, for instance, Industry Canada and other government departments have viewed the Internet not only as a tool for communication, but also as a tool for improving the Canadian economy; hence they have made as many efforts as they can to make electronic channels more appealing to Canadians.

Many of the first users of the Internet, who envisioned it as a means of communicating with people that share their interests regardless of nationally drawn borders, believe that the Internet is a bastion of freedom that would be ruined by the hands of law makers (Lessig, Shapiro, Levine, et. al.). Others believe that the Internet no longer exists as it did when that vision of unfettered freedom of communication existed (Bensen)³¹. Instead, they believe that the Internet now embodies corporate ideals, consumerism, information access sites, pornography, hate propaganda, chat rooms,

³¹ S.P. Benson. "Village People? The Net Generation" IEEE Communications Magazine. Jan 1998. pp. 32-35. Vol. 36, No. 1.

newsgroups *and* other personal communication tools (Milojicic)³². The Internet has become much more than its originators claim it was created for. One cannot help but believe that barring failure, it was always expected that the Internet would be transferred from the public sector to the private sector. This is especially true when we consider that when the domain name system was created, “.com” was created for commercial use only, which at the time was strictly prohibited from the Internet. It is likely that the vision that the Internet’s creators had was a vision much greater than just military use. It is likely that the creators of the Internet envisioned a tool that would allow people to communicate across borders, platforms, languages, and cultural barriers. While this has come true to some extent, there is still a long distance to travel to achieve a seamless, safe, and all encompassing communications tool. In fact, many global citizens have yet to make their first phone call, let alone use a computer to communicate and purchase from electronic economic channels around the globe.

Seducing the Powerless with Power

It is recognized that there are intrinsic problems involved with leaving the Internet to govern itself. Left to its own devices, the Internet may become a perfect tool of control. It may be a boon for chaos, such as that that was found in William Golding’s Lord of the Flies. In Golding’s novel, boys who become stranded on a tropical island become hungry for power. Chaos and murder ensue in an effort to illustrate the necessity of civilized governance. To resolve some of the chaos that currently exists with the Internet as a communication medium, law professor Lawrence Lessig suggests that a constitution to establish “values that a space should guarantee”, be somehow instituted to

³² Dejan Milojicic. et al. “Trend Wars: Internet Technology” IEEE Concurrency. January-March 2000. pp. 70-81. Vol. 8, No. 1.

add control, privacy and continuity to cyberspace. He suggests that code could be layered onto the existing platform of the Internet to help law enforcers and policy devisors establish a viable communications framework on the Internet that would offer the chance to track and punish electronic crimes. Just as Canadians do not want the government to know where they take their cars when they leave their home, or the phone company to track the details of their personal discussions over the telephone, they do not want their electronic journeys tracked. They would not want tools imposed upon them that reveal information such as your age, province of residence or your sex. Online retailers and consumers are currently enjoying an unfettered market over the Internet largely because regulatory bodies, such as the CRTC have openly stated that the Internet will thrive best if left to its own devices. Many critics believe that the statement the CRTC released in May of 1999 was issued to mask the fact that the CRTC was in no position to establish Internet governance. Lessig's theory poses a potential solution to the problem of the regulated electronic marketplace. Whether Lessig's theory of layered control would be applicable or not has yet to be debated; however there is a strong suggestion that some members of the digital community would reject the Internet should it fall under a strict regulatory regime.

Despite the possible aversion to the Internet should surveillance tools be set in place, the future success of the Internet rests with ensuring global success in the information-based economy through the enactment of various education, security and policy measures. Canada's plan includes increased post-secondary education enrollment in technology programs, tax relief for research and development as we have already seen, and new policies that are intended to ensure that Canadians using the Internet for

commerce will be afforded the greatest intellectual property and personal privacy protection possible.

The Personal Information Protection and Electronic Documents Act

There is no definitive means of answering the problems of intellectual property rights protection, just as there are no definitive means of answering to the problems of personal privacy over open electronically mediated channels. As the onslaught of the Internet has raised serious concerns by all parties who use it, the federal government has taken some steps to ensure protection where it can. In the throne speech of 1999, the federal government vowed to re-introduce legislation to protect personal and business information in the digital world and to recognize electronic signatures. The government kept its promise and on April 13, 2000, Bill C-6 received royal assent in the House of Commons. The Bill, also known as the *Personal Information Protection and Electronic Documents Act*³³, (PIPED) came into force on January 1, 2001. Though it comes later than expected, the language of the Bill is intended to be neutral enough to remain valid for a few years. It is expected PIPED will be reviewed regularly and amended as needed.

One of the problems that hinder the success of e-business and e-commerce at this point is the protection of privacy. The federal government has taken steps to attempt to ease the concerns of users through the enactment of Bill C-6. Part 1 of the Bill establishes a “right to the protection of personal information collected, used or disclosed in the course of commercial activities, in connection with the operation of federal work, undertaking or business” (PIPED). Much of the Bill is based on proven practices already in place in the private sector. It is expected that members of the private sector who do

³³ Government of Canada. Parliament. Bill C-6: Personal Information Protection and Electronic Documents Act. Ottawa: August 7, 2000
 [<www.parl.gc.ca/36/2/parlbus/chamb.../bills/government/C-6_4/90052e>](http://www.parl.gc.ca/36/2/parlbus/chamb.../bills/government/C-6_4/90052e).

not already adhere to similar proven practices will begin adopting the provisions of the Act in their daily business operations as soon as possible to exercise a smooth transition when the Act comes into full force on January 1, 2003.

Through the Act, anything that the government can accomplish on paper can now be accomplished electronically. This provision allows the government to move into the delivery of its services electronically without contravening any other federal Acts. As the use of paper has increased by approximately four hundred percent since 1996, the introduction of measures to deliver information and services over the Internet within governmental departments and to the public is expected to reduce redundancy as well as the environmental side effects associated with the overuse of paper products.

The “Personal Information Protection and Electronic Documents Act” also establishes principles governing the collection of personal information through electronic means. These principles include

accountability, identifying the purposes for the collection of personal information, obtaining consent, limiting collection, limiting use, disclosure and retention, ensuring accuracy, providing adequate security, making information management policies readily available, providing individuals with access to information about themselves, and giving individuals the right to challenge an organization’s compliance with these principles. (PIPED Introduction)

These principles are designed to make businesses accountable and more responsible when collecting personal information electronically while at the same time allowing consumers the opportunity to repudiate and have corrected any personal information that is incorrect. The Bill ensures consumers that “an organization is responsible for personal information under its control” (Schedule 1, sec. 5, par. 4.1). This means that they are

responsible for the accuracy and safe storage of personal information and they are required by law to amend any information that is not accurate. Furthermore, by 2003 all businesses that collect personal information will be required to have an official privacy policy governing the collection and use of personal information. The Bill states that personal information must only be collected through clear and lawful means – it must not be collected through deceitful practices. In other words, businesses and organizations will only be legally permitted to collect information for the necessary purposes of carrying out explicitly defined electronic transactions. Information may not be collected or used without permission for uses other than those stated at the time of collection. Organizations will also be required to designate an individual or individuals to oversee the organization's compliance to the Act. Organizations will be required to document the purposes for the collection of personal information before or at the time of collection. These steps are designed to ensure accountability to consumers. They are also designed to ensure that consumers have a means of grieving information that is collected about them that may be false, incorrect, or misused. It establishes a clear path for the correction of incomplete or incorrect records. When an article of personal information has not been amended by the organization in question, the consumer may appeal to the Privacy Commissioner to intervene on their behalf and force the amendment or ensure that the problem is duly noted in the client's record.

The Act has been designed using neutral language in order to retain validity despite changing technologies. For this reason, it is unlikely that the concerns of citizens will be vastly different in 2006 when the Act will be reviewed. Consumer concerns regarding the collection of their personal information will continue to be an issue. The

Act comes at a time when consumers will most need the support of government if they are to take advantage of the technology drivers of the information-based economy.

While the PIPED law has taken clear steps to make the electronic marketplace more accountable to consumers, it does not take steps to legislate criteria for the establishment and maintenance of best practices for third party Certification Authorities (CAs). Certification Authorities are “trusted” third parties responsible for the distribution of public keys in open cryptography networks (discussed below). Their role is essential to the maintenance of open network security in the transmission of personal information. In October of 1998, the Government released its official policy on cryptography and Certification Authorities. The policy outlines how the federal government intends to ensure consumer privacy during electronic transactions without legislating licensing criteria for CAs. The Federal Government has turned its support to an industry-led accreditation system for private-sector certification. Federal policy-makers believe that the public and private sectors should work collaboratively to establish criteria that are appropriate for accrediting CAs. The reasons for establishing accreditation criteria include:

- to provide a means for users to establish the trustworthiness of certification authorities;
 - to establish a consistent and auditable lever of trust of authentication schemes;
 - to allow for users to make choices based on some known parameters for trust and confidence; and,
 - to minimize situations where businesses and consumers, involved in more than one authentication scheme, may be faced with differing (and potentially even conflicting) requirements.
- (Building Trust, 8)*³⁴

³⁴ Government of Canada. Electronic Commerce Branch of Industry Canada. Building Trust and Confidence in Electronic Commerce: A Framework for Electronic Authentication in Canada. Ottawa: 2000.

It is essential that consumers have a means of ensuring their privacy is protected when they conduct transactions on an open network such as the Internet. As it stands, Bill C-6 legally allots the protection of personal information, but it does not establish a means of verifying a legitimate business from an illegitimate one. Furthermore, it is unlikely that the federal government has the financial means to enforce the Bill. Effectively enforcing the Bill would be costly and given that the government has often fallen short on promises to move forward with becoming the most connected country in the world, critics anticipate that they will not follow through on the strict enforcement of the Bill that citizens have called for. Consequently, the Bill will fall short of its goal of establishing a means of ensuring that the public has the greatest privacy when transacting business online.

It is doubtful that the federal government or any other public governing body would be able to establish a regulatory means of ensuring privacy to all members of the public, which further complicates matters outlined in the Bill. Instead, the future is more likely to witness a transition from federal policy legislation, to private policy practice. This will be done through the use of code modifications, digital signatures, strong encryption practices, third party certification, intrusion detection, computer forensics, and reliable software.

Technology versus Technology

The limited ability of federal regulators to bear any control over the content and circulation of electronic data over the Internet has prompted private organizations to regulate the dissemination of intellectual property over the Internet with their own technologies. Encryption, authentication, digital signatures, intrusion detection,

computer forensics, reliable software, wireless security and other new techniques are of paramount importance to corporations who want to protect their digital assets. There are, however, some concerns over the application of intellectual property protection technologies. Some users are concerned that protection technologies will give “content owners so much control over their material that research scientists, students, journalists, and others will lose the access to intellectual property for academic and public-interest purposes” to which they previously had access (Lawton, 14)³⁵. The tightening commercial restrictions of intellectual property rights and the rights of fair use have not gone unnoticed; however, as yet, there have been no solutions that offer a viable alternative to the restrictions that privacy protection technologies place on intellectual properties.

Content retailers that have not already implemented encryption programs will soon begin implementing encryption programs that require the user to access on-line authentication. This will be done through the use of trusted systems – devices or applications that “can be trusted to follow usage-limitation rules implemented by content owners” (Lawton, 14). Vendors generally “implement intellectual-property protection by inserting machine-readable tags in the content” (Lawton, 14). There are already products on the market designed to certify ownership on-line through the use of a trusted device. If Canada is to continue to be a world leader in the realm of high-speed Internet technologies, it should consider investing research and development funds into the creation of security software designed to help protect the interests of producers and users of copyright materials, while at the same time insuring the rights of fair use that are set

³⁵ George Lawton. “Intellectual-Property Protection Opens Path for E-Commerce”. Computer, Feb. 2000, pp. 14-21. Vol. 33, No. 2.

out in Canadian copyright law are upheld. The rights of fair use authorize limited use of copyright protected materials for the purpose of public critique, academic and journalistic research.

We must be cautious with the use of trusted systems that are designed to verify ownership. Andrew Shapiro writes that trusted systems

monitor information use in a way that could jeopardize our right to privacy with regard to what we read, listen to, and watch. Each time you look at a picture online that is protected by trusted systems, for example, a computer somewhere takes note of that action. Under the guise of making sure that protected works are not used in an unauthorized manner, trusted systems could become perfect surveillance tools. (82)

The use of protective technologies in no way assures users' privacy or freedom from surveillance, because these tools are designed to be instruments of surveillance. They are designed to monitor legitimate ownership. To do this, you must somehow register your legitimate ownership with the trusted system, which in turn repeatedly checks to see if you are who you have previously claimed to be and if you have the right to use copyright protected materials. Therefore, the resolution to intellectual property protection issues raised by the use of technology is found in the creation of additional, counter-active technologies.

While Canada's legal system assumes innocence until guilt has been proven, trusted system technology functions in the opposite manner, assuming guilt until innocence is proven. An embedded trusted system automatically assumes theft of intellectual property, and then takes steps to prove ownership. Yet, there are advantages to investing in and using the current trusted system technologies. As there are currently no other means of ensuring proper ownership of intellectual property sold over

electronically-mediated channels, it would be wise for private corporations and the federal government to begin an intellectual property protection initiative by implementing the technologies of companies such as SoftLock, IBM, SDMI and InterTrust. “Machine readable tags written into plug-in intellectual-property protection technology from SoftLock.com can instruct players to restrict an individual’s ability to copy, save, cut and paste, or otherwise use a specified Adobe Acrobat document in unauthorized ways” (Lawton, 15). This is already in use in many corporate electronic libraries. SoftLock’s method of protecting documents and other forms of intellectual property would require the user to have an always-on connection to the appropriate authentication site in order for the user to have access to software of which he or she has legitimate ownership. This poses a problem to users who do not have such access or cannot attain such access due to financial or geographic limitations.

IBM’s Cryptolope works in a fashion similar to that of SoftLock.com’s protection. Cryptolope wraps protected content with Java-based encryption.

When a user tries to access the content, either initially or subsequently, the Cryptolope communicates via the Internet with an authentication server. The server verifies the user credentials required to access the product. (Lawton, 15)

Again the user must have access to an always-on Internet connection, when using copyright-protected software in order to retrieve user authentication from the verification server. A user may not implement a computer program that is protected by a trusted system until he or she verifies ownership with the authentication server.

The SDMI product, which uses embedded strong watermark technologies, also requires an always-on link to the Internet. Digital watermark technologies work much the same way that watermark technologies on security documents work. A digital tag is

inserted into the code of the product and is then retrieved and verified by the server authentication site. InterTrust's DigiBox does not require the user to have an always-on connection, though a continuous connection would enhance the functionality of the required intermittent verification of user authorization. The DigiBox works by downloading server authentication onto the user's machine. "The server then checks occasionally via the Internet with a transaction authority server" to charge users' accounts and to make sure that accounts are paid in full (Lawton, 26). Ensuring that users are protected from privacy invasions by producers of intellectual property who are necessarily concerned for the fair use of their intellectual property is a challenging dilemma. Counter-active technologies are likely the only solution to the problems that open technologies have posed to date. Therefore, issues raised by technology are most likely to be resolved with the creation and implementation of more technology.

Code is the most significant means of regulating any or all parts of the Internet. Code is bits of data that determine how a piece of hardware, or software functions. Change the code embedded within the system, and you change the system. The incredibly flexible nature of code allows for seamless and instant changes in the system. It also allows for electronic regulation of Web services, the creation of new software, and the invisible layering of control onto the platform of the Internet. Law professor Lawrence Lessig believes that "*architectures of control* could be layered on top of the Net to 'correct' or eliminate 'imperfections' of control. Architectures of credentials and architectures that label could... facilitate architectures of control" (29). This is theoretically achievable; however, whether consumers would still be willing to conduct business and converse over the Internet if there was more control has yet to be debated.

The Internet has thrived largely because it has been untouched by regulatory bodies. If government were to step in and begin legislating architecture technologists to write control code into their software and hardware devices, there could be a strong backlash against the federal government for intervening in the open market and restricting personal transactions. As the federal government believes that the Internet is essential to belonging to the global community, the only regulations that it would be wise to make would be those that enable better access to the international market and those that protect the rights of Canadians when transacting in Canada (as we have already seen). If the federal government were to initiate regulation of the Internet, it would have to be orchestrated on a third party level. For example, the government could legislate that only certain types of encryption, technical devices and like products could be produced for export. Reducing the market share of a product by effectively removing it from international trade limits the likelihood of producing a product that the government is opposed to without actually placing restrictions on the content or design of the product. Therefore, while code regulates the Internet, the government has a means of regulating which code it allows for export. This type of action exercised by a government limits the power of businesses and the individual and reinforces the power of the state. At this time, the Canadian federal government has stated that it will not “restrict the freedom of choice of individuals or businesses to import or use cryptography. Users are free to determine what kinds of authentication and encryption products and services they need” (*Electronic Commerce Strategy*, 24)³⁶. While Canada does not restrict the internal use of cryptographic technologies, it does maintain its role, along with thirty-two other

³⁶ Government of Canada. Electronic Commerce Branch of Industry Canada. The Canadian Electronic Commerce Strategy. Ottawa: 1999.

countries, to monitor which products require export permits and which do not (*Electronic Commerce Strategy*, 24). The Canadian federal government thus acts as a third party legislator of technology production by limiting the international distribution of encryption and security products. While it may be true that there are countries that would benefit from the use of strong encryption and security products, restrictions are placed on the export of such products to protect Canadians from would be thieves, assassins and criminals.

Intellectual Property Rights and Privacy Protection Technologies

As intellectual property and privacy rights receive more public attention, users and producers alike become more aware of technologies they can use to take precautions against abuses of their personal property and personal information. These technologies range from simple and unobtrusive, to complex, and highly effective. The most commonly used technologies include symmetric key encryption, public key encryption, weak encryption, strong encryption, digital signatures, password protection, intrusion detection, third-party certification and computer forensics.

Encryption

The purpose of using encryption techniques is to render a message unreadable by anyone who does not hold the key to open it. Encryption has been around since the time of the early Roman Empire. In the time of Julius Caesar, a rather crude system of encryption was used when orders were sent to generals on the battlefields. "It involved shifting the letters of the alphabet a predetermined number of characters" (*Encryption Explained*, 1)³⁷. At the time, this method would have been considered state of the art. In

³⁷ "Encryption and Digital Signature Explained". Entrust. Canada, 1996.

fact, that same method was used to varying degrees for centuries. The system of moving characters required a key to unscramble how the characters had been moved so the message could be read. The same key was used to scramble the message as was used to unscramble. This process is known as symmetric key encryption. “A symmetric key system is a set of rules for transforming your original plaintext message into its coded version, the ciphertext” (Richardson, 116)³⁸. The ciphertext is more difficult, but not impossible to decipher without the key that was used to encrypt it.

As the keeping of state secrets became more important, mathematical means of delivering encryption services became more common. This system was more advanced than the character shifting system of Caesar’s time. What remained necessary however was the need to send the decrypting key along in a separate message so that the encrypted message could be decrypted. There are at least six symmetric key encryption algorithms that are commonly used in current security processes: The Data Encryption Standard (DES), Triple DES, The International Data Encryption Algorithm (IDEA), Blowfish, Twofish and RC4. Among those, there are stronger versions. The International Data Encryption Algorithm “uses a 128-bit key” to encrypt data (Caloyannides, 41)³⁹. It is used in programs such as Pretty Good Privacy (PGP) and Speak Freely, a program that allows digitized voice traffic to be sent over the Internet.

Blowfish is a 64-bit block code that has key lengths of 32-448 bits (Caloyannides, 41). It is known as one of the best available algorithms because it delivers a variable key length that adds extra security to the data being encrypted. It is recognized for its

³⁸ Robert Richardson. “Public Key Infrastructure.” Network Magazine. June 2000. pp. 114-120. Vol. 15, No. 6.

³⁹ Michael A. Caloyannides. “Encryption Wars: Early Battles”. IEEE Spectrum. April 2000. pp. 37-43. Vol. 37, No. 4.

strengths and is widely used in over 100 products. As it is considered a strong encryption technology, its use is limited to countries that are permitted to use strong encryption under the Wassenaar Arrangement⁴⁰. Twofish is also known as a strong security product that delivers long encryption strings to encrypted data. It is being considered as a 2001 replacement for DES by the Advanced Encryption Standard (AES).

Perhaps the most complex symmetric key algorithm is the one used in RC4. The RC4 algorithm is “a stream cipher of unknown security...[that] adds the output of a pseudorandom number generator bit by bit to the sequential bits of the digitized plaintext” (Caloyannides, 41). This means that the algorithm generates a variable that alters the sequence of bits encrypted that makes decryption without the matching key next to impossible.

Public Key Encryption

The most common form of encryption used by business, consumers and the federal government today is public key encryption. Public key encryption requires the establishment of a public key infrastructure, or PKI. A public key system differs from a symmetric key system because the same key is not used to encrypt the message as is used to decrypt it. Public key encryption requires that each user in the system create two separate keys. The first is used to encrypt the message. The second is used to decrypt the message. When the encryption key is used, it creates a digest hash that can only be decrypted by the matching key, which uses a different algorithm to produce the same

⁴⁰ The Wassenaar Arrangement has been established in order to promote greater responsibility in transfers of conventional arms, dual-use goods and technologies in an effort to prevent destabilizing accumulations. Through national policy, all participating states ensure that transfers of these items do not contribute to the development or enhancement of military capabilities or states identified as unstable or confrontational <<http://www.wassenaar.org/docs/index1.html>>

digest hash to unlock the contents of the message. With PKI, the user keeps his or her secret key discreet, and makes the decrypting key public. The key held in secret is known as the private key and the key that is shared is known as the public key. As different keys are required to encrypt and decrypt the message, revealing the public key does not compromise the secrecy of the message.

Public Key Encryption was first proposed in 1976 by Stanford professor Martin Hellman and his graduate student, Whitfield Diffie. The widespread use of public key encryption ensures that users will have more protection when sending and receiving messages, orders and other sensitive materials. There are at least two strengths of public key encryption that are used commonly. Hellman and Diffie's scheme allows the recipient of a message to verify that the sender is who he or she claims to be and that "the message has not been tampered with" (Caloyannides, 40). The system works best when both parties have the same software to create a pair of keys. The sender makes known their public key by posting it on the Web or by sending it in an email to the intended recipient.

Integral to the usefulness of public key encryption is the verification that the message is authenticated. To do this a user may perform what is known as a cryptographic hash function.

The hash function compresses the bits of the plaintext message into a fixed-size digest, or hash value, of 128 or more bits. It is extremely difficult to alter the plaintext message without altering the hash value. (Caloyannides, 40)

Another feature of public key encryption that adds value to its use is that one key cannot be mathematically deduced from the other key. Each key will produce a different digest

hash that in no way resembles the other, thus leaving no means of determining what the encrypting key is comprised of.

All encryption involves an algorithm that produces a string of randomly selected numbers used to encode the message (Caloyannides, 39). Generally speaking, if the string is shorter, the encryption will be weaker, and more prone to penetration, thus presenting a greater security threat. If the string is longer, the encryption will be stronger and far less penetrable.

Generating a public key can be time consuming when files are large. For this reason, the widespread use of symmetric key encryption will continue. Not only does symmetric key encryption add security to ciphertext, but it also enhances the operating speed of public key encryption. To do this, users first encrypt their message using a symmetric key. This process compresses the text, or data of the file, thus rendering a smaller plaintext for the public / private key to encrypt / decrypt. The public key is then used to encode the local key, and both keys are sent to the recipient. This process not only saves time, but also adds security to messages that are sent over open networks where security cannot be guaranteed.

Strong encryption techniques are clearly good for business and government. They increase privacy and opportunity by functioning well over open networks. Governments, however, are concerned that the use of strong encryption techniques will severely limit their ability to monitor and decipher electronic crimes, which on average tend to leverage a much greater return than non-electronic crimes, for example bank theft. Members of the public as well as businesses clearly have the right to ensure their own security. The greatest concern for federal regulators, however, is that they will not be able to decipher

information to which they would previously have had access. In the past, law enforcement officials could petition the courts to gain access to the information stored in people's homes, or to overhear their phone conversations via search warrants and wiretaps. Now, law enforcement officials cannot gain access to files on computers that are protected with strong encryption techniques. Consequently various governments around the world are trying to find a solution to the problems of deciphering encrypted files on the computers of suspected criminals. In the United Kingdom, a law has been passed that requires the suspect to render the key to officials. The idea works well if the suspect is cooperative, or if there is a suspect in custody at all. It fails in the event that that suspect is uncooperative or unavailable. Alternatively, Canada has stated that it will not restrict the use of cryptographic technologies within its borders. Canadians may purchase, design and use any cryptographic technology they choose. They may not, as we have seen, export cryptographic technologies that are regarded as international security risks.

Encryption does not ensure that a file is completely protected from penetration, theft, or interception, but it does ensure any changes in the original message can be detected. Verification that the digest hash has not changed from the time the file was sent until the time it was received and opened by the recipient ensures that the security of the file has not been breached. There are also those whose occupation it is to hack and break strong cryptographic technologies. While the breaking of encryption is extremely time consuming, it can most certainly be done and we would be foolhardy to believe that the use of a 2304-bit public key algorithm will continue to be unbreakable. As computer processor power continues to advance, so will the ability to augment cryptographic

powers increase and so will the use of faster computers to disable cryptographic technologies increase.

Digital Signatures

Along with encryption technologies, digital signatures offer effective security to users. Canada's federal government issues digital signatures for most of its employees. They are used to validate that the sender is who he or she claims to be. A digital signature is a "bit of text that tells something about someone or some server on the network" (Richardson, 114). A digital signature should say what the users' name is, or that they are authorized to be on a restricted page because of their age, or that they are authorized to purchase goods via the Internet on behalf of their organization, or that the site that they are communicating with really is the site it claims to be. In most cases a digital signature remains on the users computer. Typically a digital signature is signed using a private key. Verifying the signature requires the recipient to verify that the public key matches the private key and the signature belongs to whom it is purported to. In many cases, the signature belongs to a Web site selling goods. It is the consumers' means of verifying that their information is being kept secret and that they are on a secure network. This is referred to as a Secure Sockets Layer, or SSL.

Of concern to companies and government is who should be issued digital signature certificates. In the world outside of cyberspace, government and security document producers such as the Canadian Bank Note Company issue tamper-proof documents. These are organizations that are authorized to produce documents and certificates that verify you are who you claim to be. In most cases, documents such as passports and drivers licenses have the bearers photograph on them, visually linking them

to the documents and the facts stated thereon. In cyberspace, however, there are no physical facts linking you to the person you claim to be. The issuance of digital signatures authorizes organizations and individuals to transact in cyberspace while at the same time proving that they are who they claim to be. A digital signature typically uses PGP because it has been more rigorously reviewed and tested than other algorithms. To date, it is the safest means of verifying digital signatures.

Password Protection

While it is extremely important to ensure that files, messages and personal information are protected during online exchanges, it is also important to ensure that data on hardware and software are protected from penetration. As consumers, businesses and governments move into the information economy, the information that they store and sell becomes more of a commodity than it has ever been. Protecting that commodity from theft is important. Intellectual property stored on hard drives, compact disks, digital audiotapes, zip disks and floppy disks are equally prone to theft by nature of their mobility. A simple means of protecting intellectual property is to lock the information with a password. Password protection is by no means a perfect way of ensuring safety, but it will help against intellectual property theft. As long as the password is kept secret, the security of the file system will be protected. If the password becomes known, however, all security safeguards are lost. The best recourse is to change passwords frequently to avoid detection. Furthermore, passwords should not be comprised of names and numbers that would be obvious to would be thieves. The disadvantages of password protection can include cost and the “inconvenience of continually using passwords to move from one space to another” (Lessig, 34).

Intrusion Detection

In the event of a computer or network violation, Intrusion Detection programs can protect many businesses and consumers from intellectual property theft. Would be thieves, hackers and other electronic criminals often enter networks through loopholes and through gateways that are more easily penetrated than other entrances might be. It is extremely important to protect from unlawful entry through the use of the technologies we have already discussed. In the event that these technologies fail, however, it is important to have a means of detecting intrusion and ousting the intruder as quickly as possible. Intrusion detection software works by notifying the user, or network administrator if the integrity of the encryption or protective devices have been in any way compromised. Businesses and consumers will have different means of responding to intrusions. Notification of intrusion is integral to the prevention of further attacks as it illustrates to administrators and users alike where there may be weaknesses in the system.

During the second week of February 2000, there were a series of attacks launched against Internet giants such as Yahoo, CNN, Amazon.com and eBay. These attacks brought the service of these sites to a halt while never intruding the servers that upheld the sites. The type of attack that took place is known as a Denial of Service (DoS) attack. Denial of Service attacks occur when a hacker mimics the Internet Protocol addresses of thousands of users and then bombards Web sites with thousands of illegitimate requests for services or information, thus making it impossible for the system to respond to legitimate requests. A DoS attack exploits the weaknesses of the TCP/IP standard used on the Internet. This attack does not steal or modify any of the information on the affected system. They are used only to disable a system; therefore, in such instances

strong encryption and intrusion detection software will not prevent an attack. In fact, there is no known prevention against a DoS attack at this time. Instead, governments and users suggest that enterprises track traffic in cooperation with Internet Service Providers to prevent IP mimicking techniques (*Technology's Inescapable Inabilities*, 18)⁴¹.

Cooperation with ISP's is part of the Canadian Association of Internet Providers (CAIP) agenda for fostering confidence in the electronic marketplace. They believe that ISP's should hold responsibility for the traffic that is carried over their networks. In an effort to uphold high standards for Internet Providers, CAIP instituted a voluntary code of conduct in 1997 that its members are expected to adhere to. The code can be found at the CAIP web site⁴² and it outlines some important industry steps that need to be taken if privacy and security issues are going to be dealt with.

In particular, the CAIP code of conduct notes that all members who adhere to the code will not knowingly host illegal content or network abuse. The code cites that Internet Providers are unable to monitor all content – consumers would not want their personal content monitored; however, investigating legitimate complaints about alleged system abuses is by no means beyond the scope of ISPs. Therefore, CAIP members and even ISPs who do not belong to CAIP typically attempt to uphold personal privacy while maintaining control over their networks and cooperating with authorities whenever possible.

Computer Forensics

⁴¹ "Technology's Inescapable Inabilities". The Monthly Research Review. March 2000: 1-2. GartnerGroup.

⁴² www.caip.com

Law enforcement officials are particularly concerned by the difficulty they have encountered when investigating alleged crimes that have involved the use of computers. Unlike phone lines, for which they can petition the courts for a wire tap and unlike hard evidence for which they can petition the court for a search warrant, computer violation protections can be much harder to detect. Furthermore, it is next to impossible to tap Internet transactions without the recipient detecting that the information has been tampered with. Computers pose a particularly troublesome problem when they are linked with crime investigation. Consequently, many law enforcement agencies employ computer specialists and computer systems that are capable of disabling encryption systems that protect data that could incriminate. The problem with this process is that it is typically very slow when alien systems and / or computer specialists are trying to dismantle strong encryption technologies on confiscated computers.

To remedy some of the problems that computers have posed during crime investigations, the United Kingdom proposed a law that requires “every operator of a ‘telecommunications service’ to incorporate facilities that allow the government to log and monitor all online activity” (Dorman, 104)⁴³. The purpose of the incorporation of a surveillance tool is to ensure that where crimes are being committed, there are means of discovering those crimes and using the appropriate legal structures to charge criminals for committing electronic crimes. The bill, which has not yet received royal assent, is called the “Regulation of Investigatory Powers (RIP) bill”. The RIP bill also governs encryption: “any computer user who possesses encrypted material must turn over the key to the police, if requested” (Dorman, 104). This is an excellent means of quickening the

⁴³ Andy Dorman. “Internet Indiscretions.” Network Magazine. June 2000. pp.100-104. Vol. 15, No. 6.

pace of computer-mediated crime investigation; however, it requires users to turn over encryption keys that they may or may not have. For instance, a user would not have the key to a cookie that had been placed on their computer by a web site they visited. Under the RIP bill, they would be compelled by the law to turn over all keys, including keys to cookies. The proposed law states that not having the key is no defense. Writer Andy Dornan notes “users will have to prove that they were never in possession of the key. This concept runs contrary to the basic legal principle that people are innocent until proven guilty” (Dornan, 104).

While the RIP bill attempts to ease the difficulties associated with computer-mediated crimes, it falls short of ensuring citizens the rights that they are guaranteed through other laws. Also of importance is whether or not there really are any viable responses to the problems posed by computer-mediated crimes. As it is written the RIP bill does not allow for external access to a users computer – a capability that is written into the code of the Net.

Secure Wireless

The open channel nature of wireless technologies, combined with the infancy of these services necessarily makes it sensitive to security breaches. Given the early development and deployment stage, coupled with the general distrust of wireless technologies, security for wireless devices, such as cell phones and personal digital assistants is essential to increased adoption rates. Unfortunately security for wireless devices data transmissions is limited at this stage, though there are advances being made. Currently, the market consists mainly of PKI and certificate authentication over wireless, though the partnering with providers of both wireless and security providers is also

limited at this stage of development (King, 2)⁴⁴. In addition to the offering of PKI and certificate authentication at the device level is the growing concern over user authentication. Given the size and easy theft of mobile devices (98% of businesses have reported theft of mobile devices), the issue of user authentication for government, business and personal use is of growing concern (King, 4). In an effort to ensure the authentication of the user and the device, some providers have responded by creating applications that are Personal Identification Number (PIN) dependent. This method ensures that the user is who he or she claims to be as the PIN is kept confidential and can only be identified by the system receiving the information. Also commonly implemented is Wireless Transport Layer Security, which is an adoption of the Secure Socket Layer for wireless communications (Crouch, 1)⁴⁵. In addition to the implementation of stronger, more effective security techniques for wireless devices, the implementation of security procedures across the entire network and an increase of bandwidth necessary for the data increase that improved security requires must be added in order for wireless security to become more effective.

As we have seen above, there are many measures currently being undertaken to ensure proper ownership of intellectual properties as well as legal conduct over the Internet and over open computer-mediated information systems. At this time, it is unknown what shape the technology will take or to what extent the effect of new information collection and management laws will have on the success of the Internet marketplace and on the success of ensuring consumer privacy is upheld. Yet, we cannot help but be either mesmerized or completely disenchanted by the technologies that are

⁴⁴ Michael King. "Mobile Security: Steps in the Right Direction". United States: Gartner, Inc., 2001.

⁴⁵ Cameron Crouch. "Experts Ponder Securing the Wireless World". PC World.com. April 11, 2001. <www.pcworld.com>.

taking a firm hold on the way that we conduct our personal and professional business.

Regardless of our reaction to the software tools that are governing the means of interaction over the Internet, there can be no mistaking that the private sector and the technological innovations that they implement to control who uses what will shape the Internet in the years to come.

Summary, Conclusions and Implications

Summary and Conclusions

The growing use of technologies has largely aided and abetted the success of the Internet and its seemingly required adoption for the Canadian Government, Canadian Businesses and Canadian Citizens. From its early stages as a communication tool for military personnel, to its implementation in North American Universities as a tool for academic information exchange, to its role as an arbiter of a more responsible and “connected” Canadian government, the role of the Internet on Canadian society is easily perceived. The widespread sharing of information that was previously confined to warehouses and location-specific libraries has made infoglut a common issue in the lives of more than 10 million Canadians. This thesis has explored the impact that open channel communications technologies and the Internet itself have had on Canadian society at large. It has also examined some of the negative aspects of Internet-dependent communications along with the security risks associated with these communications. Many conclusions have been drawn throughout the argument that warrant review here.

In the first chapter, we examined which technologies are currently being used to connect Canadians to the Internet and which technologies are likely to be adopted in the not-so-distant future. We concluded that ISDN would not be a tool of common use, and that ADSL and the Internet-over-Cable were the most likely direction for growth of the Canadian Connectivity market in the coming 3-5 years. We also concluded that these technologies, though fast for our needs at this time, will soon reach the end of their

lifespan as faster technologies are needed to carry the services that we will be using on a regular basis, such as VoIP and Video Conferencing.

Wireless technologies of varying natures are likely to become most popular over the course of the next ten years, given the adoption of high security standards and the adoption of common operating standards. There are obvious directions that the technologies we use for data communications will take over the course of the next ten years. Predicting them is difficult, given the level of infancy and the rate of hyper development.

In the second chapter, we examined some of the reasons why people were originally drawn to the Internet and what draws them there today. We also looked at why we need high-speed access, and the effect that the establishment of local “Internet Communities” could have on Canadian identity. We also examined, to a limited degree, what role the Canadian government was having on the adoption of Internet technologies.

Chapter Two concluded that the original attraction of the Internet was in its ability to bring disparate people together in a common forum for a common purpose: to communicate. The evolution of the medium has brought about negative aspects such as limited access, offensive content and a general tone of banality. Given the research conducted, there is evidence supporting the argument that the attraction of the Internet lies in its ability to bring people together from disparate locations and social backgrounds. The success of the Internet is largely based on its ability to reach the masses and allow for communications of common opinions, shared discussions and the elimination of visibly hindering social markers that affect regular communications environments. In addition to the removal of these markers, the ability to conduct

transactions over the Web that make our daily lives much easier has also added to its growth and attraction.

Chapter Two investigated some of the public-facing initiatives that the federal government has undertaken in the recent past and the effect that these initiatives are expected to have on the Canadian public. We noted that the *Connecting Canadians* initiative was expected to thrust the importance of the Internet on the lives of all Canadians. At this stage, we can conclude that the implementation of *Connecting Canadians* has affected the perception that Canadians have about the Government's ability to adopt technology for the improvement of Citizen-to-Citizen communication.

In the second chapter, we noticed that the adoption rate of e-business transactions has increased dramatically and is now starting to impact the overall acquisition transaction rate for Canadian households and businesses. The impact of e-business and electronic transaction processing is expected to increase dramatically over the course of the next 5-10 years as security standards increase and as the elimination of paper-based transactions begins to take a firmer hold on businesses.

The third chapter looked at how three federal departments are changing the way that they operate internally to improve external services to citizens over electronic channels. We concluded that Statistics Canada has to make changes to its strategies in order to achieve success with its electronic channel. This is due to the fact that they have failed to update their back-office systems – an update required for a more complete and holistic approach to electronic transaction processing and information sharing with its constituency. The Department of Foreign Affairs and International Trade, we concluded, has the most holistic approach to the strategic implementation and transformation of the

way that they conduct their business, both internally and externally. For this reason, it is believed that the success of DFAIT's approach to electronic transaction processing and electronic service delivery is likely to be a high, but only given proper funding.

Canada Customs and Revenue Agency has an approach to electronic service delivery that differs from both Statistics Canada and DFAIT, in that they have a high level of risk associated with the possible breach of their systems. Ensuring extremely strict levels of security is the first step to ensuring successful adoption of electronic transaction processing at CCRA. This is due to the fact that this department in particular touches the lives of all Canadians, either directly or indirectly. Security is the single greatest risk that CCRA is challenged with at this time, as are all other federal, provincial and municipal governmental organizations. To achieve success with all of their programs, the barriers that currently inhibit electronic transactions must be overcome. As CCRA has been in the business of electronic service delivery for many years, the expectation for them to succeed at offering secure transaction processing is extremely high. In fact, the expected success rate of all government technology initiatives is perceived as very high by Canadians, yet the failure rate is significant and the ability to produce the services that Canadians are currently demanding is extremely limited by government budgets and tax payer contributions.

In Chapter Four, we carefully examined some the initiatives that the Canadian Government has undertaken to transform Canada into the most connected country in the world. In particular, we examined the Personal Information and Electronic Documents Act, which has been designed to protect Canadians in Internet space before, during and after transaction processing. We also concluded that while the review cycle of the Act is

exceptionally long, (given the rate at which technologies advance at this time,) the government has evidence that indicates that the needs of Canadians will not likely change dramatically during the 5 year review intervals. We concluded that while the Act has taken steps to ensure that the privacy of Canadians is protected in cyberspace, the Act comes later than expected and does not address the issues of certification authorities accreditation and the establishment of criteria to help consumers determine legitimate businesses from illegitimate ones. Consequently, Certification Authorities will govern themselves until the Government can make amendments to the Act to reflect the growing needs of Canadians. Perhaps the most significant concern that arises from the establishment of the Act is the fact that there is limited likelihood that the Privacy Commissioner will be allotted the proper resources to ensure that the Act is closely adhered to by the private sector. Ultimately, we concluded that the Act falls short of its goal of establishing a means of ensuring that the public has the greatest privacy when transacting business online because the government simply does not have the means, and the power to govern the Internet nor the security of its citizens while they are engaged in Internet transactions.

Chapter Four also closely investigated the technologies that are currently being used in place of legislation to ensure privacy and the protection of intellectual property rights. While these technologies (encryption, authentication, digital signatures, intrusion detection, computer forensics, reliable software, wireless security) are of importance to the success of electronic transactions over the Internet, they pose a significant threat: they place governance of intellectual property in the hands of the producers. The use of technology to battle the undesired effects of some technologies clearly poses a significant

threat to the rights of fair use. Many who regularly access content in libraries and over the Internet will now either be forced to pay for information that was previously free, or their actions will be limited and monitored in cyberspace. While it is obvious that the implementation of technologies to limit or prevent theft are warranted, the limiting of the rights that citizens previously exercised is of increasing concern to the public and to legislators. We concluded, however that there was no viable alternative to the use of “solutions” that provide protection to intellectual properties and personal privacy at this time.

The curious, probing and cautious nature with which we approach Internet technologies is well warranted. It would be unwise to continue along the path of blind acceptance that marked our first approach to the adoption of Internet technologies when they began to penetrate our lives during the early 1990's. Now that we have stepped out of the fog of enchantment, we will be able to use the Internet and new technologies in ways that we had not anticipated even ten years ago. With a cautious approach to technology, there will be a measurable affect on social governance and transaction processing. The integration of tools yet to be created are what separates the vision of tomorrow's electronic channel from the reality that it is today.

Implications

Our investigations of Internet technologies, their impact on Canadian culture and Canadian governance, as well as the technologies that are being used to manage and monitor use of information technology and intellectual property exposes serious implications that warrant further discussion. The preceding work clearly shows that the federal government has stepped back from policy making in the area of the Internet. The

research herein has also made it clear that the private sector has emerged as the controlling power in the governance of the Internet. These two issues are inextricably linked and we need to examine the implications of this shift in control.

With the exception of the PIPED Act, discussed in Chapter Four, the federal government has done very little to protect Canadians while using the Internet. In addition, the federal government has allowed some of the largest corporate mergers in history to take place in the name of electronic convergence and streamlined service delivery. There is an obvious removal of governance on the part of Canada's federal government.

The federal government's self-imposed retraction from policy making in the area of the Internet is inextricably linked to the private sector's dominance of the Internet marketplace. The power that the private sector holds over the Canadian public and the federal government leaves policy makers virtually helpless. Technologies are developed outside of Canada, predominantly in the United States and are designed to operate on computer systems that are used in Canada and elsewhere in the world. The Canadian government is left with the choice of encouraging internal development of similar technologies in an effort to foster research and development in Canada, and to adopt technologies created in foreign markets. Canada's federal government is forced to take this approach or risk being left without new information technology hardware and software tools. As Vincent Mosco⁴⁶, professor of Mass Communications at Carleton University, writes,

⁴⁶ Mosco, Vincent. "Myth-ing Links: Power and Community on the Information Highway." E-Commerce vs. E-Commons: Communications in the Public Interest. eds. Marita Moll and Leslie Regan Shade. Ottawa: The Canadian Centre for Policy Alternatives, 2001. pp. 9-20.

Today, governments worried about the loss of control and businesses eyeing cyberspace as a new marketplace – as a source of new commodities and a means to repackage old ones – lead critics to conclude that history is in the process of repeating itself. Part of the process of preventing another lost opportunity is to unmask the myth that today's information highway is inevitably leading us to a new sense of community and to democratic communication. (11)

The fact that there is an overwhelming, and misguided, sentiment that the Internet is leading us to a new sense of community places the Canadian federal government in a position where it feels powerless to control the Internet in Canada. The implication of this is evident in the overwhelming control that the private sector is increasingly exerting over the Internet.

The federal government has turned its attention from regulation toward the implementation of the information technology over which it has lost all control. As we saw in Chapter Three, the federal government has made efforts to use information technologies in the workplace to enhance, simplify and expedite processes. These steps require that the government invest in information technology; and that that information technology operate in a manner that is conducive to the business of running a country. In order for the federal government to acquire technologies that it deems necessary for its daily operations, to improve or become more cost efficient, the federal government necessarily has to support businesses that may not have interests in favour of its current corporate information technology policies, acts and regulations. The tension between the federal government's perceived needs and the private sectors' wants creates a situation where the government is bullied into amending policies, acts, or regulations to favour the operation of big business in this country. Should the federal government react adversely to the demands of the Canadian and foreign private sector operating in Canada, there

could be a withdrawal of these corporations from the Canadian market place and the associated loss of work. This matter would be compounded by the fact that the federal government would likely still be unable to access or acquire the products or services they need to conduct or improve operations.

In addition to threats against the stability of the Canadian market, merger-mania has generated a much-reduced selection of media offerings in the Canadian marketplace.

In his article "Lost in Cyberspace," Carleton University professor of Mass Communications, Dwayne Winseck⁴⁷ writes that the

current revival of media reconvergence has been driven by changes in government and corporate policies that have gone from *preventing* to *promoting* convergence and concerted efforts to transform information/communication into the pivotal commodities of the "new economy" and "information societies". (Winseck, 1)(author's emphasis)

In May of 1999, the CRTC demonstrated how the federal government is backing away from policy making by announcing that it would not regulate the internet as a form of telecommunications, radio or television media. The implication of this decision was that any corporate entity that operated in the realm of Internet technologies was given *carte blanche* for their Internet operations because they were left without rules.

What does this mean for Canadians? The rapid influx of information technology into the Canadian market has effected changes that have caused a reevaluation of how business and government operate in this country. Influenced by massive mergers in United States, Canadian media giants have been pressing the Canadian federal government to reevaluate current media policy so that Canadian companies can compete with their American and global counterparts.

⁴⁷ Winseck, Dwayne. "Lost in Cyberspace" pp. 1-18

Backed into a corner, the current Liberal government has repeatedly submitted to the demands of the private sector (e.g. the recent merger between Toronto Dominion and Canada Trust.) This submissive behaviour is also generated towards information technology giants and is reflected in the federal government's approval of mergers such as CanWest Global with Southam Inc. or Bell with CTV Networks. The implication of the federal government's laissez faire attitude towards the information technology sector has been the complete redefinition of the information technology landscape in Canada. It has meant that the private sector is taking control over governance of the Canadian public – pulling the proverbial wool over our eyes by telling us that changes being made are in our best interest and by duping consumers into believing that the government supports the private sector's domination over the Canadian media landscape.

The single greatest implication of the federal government's move to back off from policy making in the realm of the Internet is the rise of the multinational corporations' dominance of our lives. As we saw in Chapter four, the power of the private sector has become the power to control what we see, what we read and what we hear. The private sector has taken control over how we use the tools. The private sector has taken to governing through the creation of new technology. The implication of this type of control is that the public is left helpless. Furthermore, many of the decisions made for consumers happens in private meetings, among standards groups and behind the doors of 'key decision-makers.' Consumers are not kept abreast of decisions that affect their choices because it is not in the best interest of corporations to inform consumers of how their choices are being restricted for the sake of increasing profit margins and satisfying shareholders.

The single greatest implication of the dichotomy brought about by “the ambiguous relationship between public and private interests: privatized and commercial interests vs. governmental regulation and control” is the loss of privacy associated with this shift in control. Many consumers believe that the private sector controls and uses information (either directly or indirectly) for self-fulfilling purposes, while the government collects or uses information for purposes of managing the country. As we saw in Chapter Three, there is a belief that some federal organizations, such as CCRA, can be trusted with personal information as they are legally obligated to do so through federal legislation.

In her paper, “Privacy Then and Now: Taking Stock Since IHAC” author Valerie Steeves⁴⁸ writes that “Personal freedom, autonomy, democratic privileges, and other general human rights do not come to us *gratis*. Democratic societies are notoriously inefficient, but we accept those inefficiencies because democracy is the best way to maintain some degree of individual freedom” (Steeves, 50) (author’s emphasis). This brings into clarity a serious implication of the federal government’s move to back off from policy making in the area of the Internet. The private sector has gained almost complete control over the area of the Internet and the degree of individual freedom. If this level of control continues to pour forth from the private sector, then its likely that the inefficient, but acceptable democratic system will be eroded to the point where governance, personal freedom, autonomy, and general human rights are accorded by the wills of multinational corporations. The “Fordism” of Aldus Huxley’s⁴⁹ Brave New

⁴⁸ Steeves, Valerie. “Privacy Then and Now: Taking Stock Since IHAC.” E-Commerce vs. E-Commons: Communications in the Public Interest. eds. Marital Moll and Leslie Regan Shade. Ottawa: The Canadian Centre for Policy Alternatives, 2001. pp. 49-56.

⁴⁹ Huxley, Aldous. Brave New World. Blah, blah blah.

World could come upon us like a beast in the night that overtakes us while we sleep.

Lulled into thinking that the corporate giant knows best, democratic society as we now know it could well be eroded by the will to control. Steeves notes that we are being confused between electronic privacy and security.

At a fundamental level, privacy is about the right to control who knows what about us – in other words, to determine what we keep within the confines of our personal lives. The trend towards ‘privacy as secured communications’ recasts privacy as an adjunct to commercial activity. (Steeves, 52)

Both rights to privacy and security have been recast in light of electronic communications in Canada. The implication of this recasting is that without clear guidance from the federal government, basic rights to privacy and security will continue to be blurred in this country.

As an adjunct to the federal government’s mass adoption of the communications technologies it seems unable to govern, there are implications associated with universal access to governmental services. The needs of Canadians who neither want nor perceive a need for the Internet have been left by the wayside. Approximately 60 per cent of Canadians who reject or are unable to use the Internet or the communications tools of the information age lose out on easy-access services such as driver’s license renewal, library book renewals, catalogue searches, access to federal government statutes and regulations, access to information about their community and much more.

Through its connectivity programs in schools, urban and rural libraries and through learning programs, the federal government is making efforts to encourage members of this group to become more versed in the tools and information available through the Internet. Yet this group remains an elusive demographic to the goal of

universal access. What the federal government is neglecting to recognize with its insistence on becoming the most connected country in the world is the fact that there are individuals who genuinely have no perceived need for the Internet or the services it brings. The government is determined to reach the members of the digital divide who cannot perceive the need for the services that have arisen with the information economy. The government is also determined to reach the members of the digital divide who are marginalized from universal access due to their residential location or financial situation. Why is there such determination on the part of the federal government to reach these two groups of un-connected Canadians? Why is there such a drive to be the first country to have universal Internet access? Beyond the thrill of international competition and the excitement of watching new developments enter the Canadian market, the answer to this question is likely to remain elusive.

In his book, Digital Capitalism: Networking the Global Market System, Dan Schiller⁵⁰ discusses in detail the changes to the corporate education system that have been brought about by the mass distribution of electronic media. He remarks that these changes have empowered transnational corporations and have consequently aggravated social inequalities. As a result of the mass distribution of electronic media, the inequalities between the wealthy, the middle class and the poor in Canada have become further pronounced. The poor are further isolated by the lack of access to the Internet, the education tools found therein and basic information that could potentially help them advance into a more solid financial situation. The digital divide is self-perpetuating in that those who have access become more educated in its uses and those who do not have

⁵⁰ Schiller, Dan. Digital Capitalism: Networking the Global Market System. Cambridge: MIT Press, 1999.

access fall further behind those who do have access. The implication of this divide is that the inequalities that currently exist between different social groups in Canada will continue to widen.

In addition to the widening of social inequalities, the digital divide has the power to create a different understanding of belonging to a social group. Due to the trajectory of computer communications, which is aimed at “reaching any individual, anywhere in the world, at any time with text, graphics, sound, video, and even smell” the ability exists to reach all the members of wealthier classes in countries around the world (Belanger⁵¹, 130). Access to these tools is limited to financial and educational means. Given that access is limited to specific social groups, there is increased chance that social identities will shift in years to come. Identity will be associated with members who belong to the connected class and the un-connected class. Given that the connected class is predisposed towards belonging to a higher income bracket, the divide between connected Canadians and un-connected Canadians becomes a divide of social opportunities. The implication then, of the divide between the 40 per cent of Canadians who have access to the Internet and 60 per cent who do not is a matter of social opportunity. Those who are connected to the Internet are afforded more social opportunities than those who are not.

Not only is access to the Internet a matter of class, but also, once users do get access to the Internet, there is an overwhelming advertising landscape aimed at providing service to wealthy, educated, predominantly white users: “the Internet itself helps to animate [the] digital divide – between wealthy, educated Internet users and poor,

⁵¹ Belanger, Marc. “Technology Organizing and Unions.” E-Commerce vs. E-Commons: Communications in the Public Interest. eds. Marital Moll and Leslie Regan Shade. Ottawa: The Canadian Centre for Policy Alternatives, 2001. pp. 129-151.

disproportionately nonwhite nonusers” (Schiller, 141). Not only has access turned in this direction, but education as well has increased the inequalities that exist between the digital divide:

Where once had existed nonprofit institutions, increasingly, there were now commercial vendors. Where once had existed relatively autonomous instructional and learning processes, increasingly, there were now attempts to cater more directly to labor markets¼ A concurrent and related reform, toward school-to-work programs, lifelong learning, and “new partnerships,” symptomized an intensifying vocationalization of the educational process. (Schiller, 144)

Essentially, the divide between non-users and users implies that the social divide that already exists will be further perpetuated by the increasing dominance of the Internet. The issue of education is increasingly what separates users from non-users. For those who have historically accessed information technology tools, they have the knowledge advantage associated with long-time use. For those who have never accessed the Internet or used a computer, the seemingly simple task of turning the computer on or accessing the Internet can be complicated and daunting. For this reason, the digital divide will continue to conquer non-users who do not have a history of using electronic media.

The digital divide, an essentially socio-economic issue, is perhaps the greatest single reason why the government’s endeavors to create a universal access system will continue to fail. Furthermore education and perceived lack of value in the tools and services that the information economy furnishes will continue to foster a difference of perceived needs and opinions. For elderly users who have managed to live their entire lives without the “advantage” of the Internet, there may be little perceived need to connect to electronic services. It is unlikely that education or money will foster a perception of need among this group. Until Canada is comprised of individuals who have

been exposed to the Internet for the bulk of their lives, the likelihood of universal access is dim. Until the private sector's control over Internet tools and content is loosened, the need for access will also be perceived as low among Canadians who are not already connected. Until the federal government concludes that the electronic revolution – much like the industrial revolution – will not be successful without good governance, the need for access to the Internet and the information economy will remain low among Canadians who are not already connected.

Works Consulted

- Abate, Janet. Inventing the Internet. Cambridge: MIT Press, 1999.
- Angel, Johnathan. "Too Many Cookies are Bad for You." Network Magazine. June 2000. pp.106-112. Vol. 15, No. 6.
- Baran, Paul. "Narrowing the Gap to Internet Access". IEEE Internet Computing. January-February 2000. pp. 49-50. Vol. 4, No. 1.
- Belanger, Marc. "Technology Organizing and Unions." E-Commerce vs. E-Commons: Communications in the Public Interest. eds. Marital Moll and Leslie Regan Shade. Ottawa: The Canadian Centre for Policy Alternatives, 2001. pp. 129-151.
- Bell, Mark. "Connectivity: Broadband rules!" Monitor. March 2000 pp. 32-34. Vol7. No. 8.
- Benson, S.P. "Village People? The Net Generation" IEEE Communications Magazine. Jan 1998. pp. 32-35. Vol. 36, No. 1.
- "CAIP Code of Conduct". Canadian Association of Internet Providers. March, 2000. <www.caip.ca/caipcode.htm>.
- Callon, Ross. "Predictions for the Core of the Network". IEEE Internet Computing. January-February 2000. pp. 60-61. Vol. 4, No. 1.
- Clark, Elizabeth. "Special Report: Privacy on the Internet". Network Magazine. June 2000. pp. 99. Vol. 15, No. 6.
- Caloyannides, Michael A. "Encryption Wars: Early Battles". IEEE Spectrum. April 2000. pp. 37-43. Vol. 37, No. 4.
- Caloyannides, Michael A. "Encryption Wars: Shifting Tactics". IEEE Spectrum. May 2000. pp. 47-51. Vol. 37, No. 5.
- Carroll, Jim and Rick Broadhead. Canadian Internet Handbook: 1995 Edition. Scarborough: Prentice Hall, 1995.
- Cohen, Danny. "Paying for the Internet in the New Millennium". IEEE Internet Computing. January-February 2000. pp. 56-58. Vol. 4, No. 1.
- Colbeck, D. "Communications Convergence". 6th IEEE Conference on

- Telecommunications, 1998. pp. 258-262. Conference Publication No. 451.
- Comerford, Richard. "Technology 2000: The Internet". IEEE Spectrum. January 2000. pp. 40-50. Vol. 37, No. 1.
- Crocker, Stephen D. "Internet-Based Collaboration in 2010". IEEE Internet Computing. January-February 2000. pp. 53-55. Vol. 4, No. 1.
- Crouch, Cameron. "Experts Ponder Securing the Wireless World". PC World.com. April 11, 2001. <www.pcworld.com>
- Curry, Ian. "Entrust Technologies White Paper". Canada: Entrust Technologies, 1997.
- DeLotto, R., Annemarie Earley, Kevin Collins. "Unraveling Some Wireless Privacy Issues". United States: Gartner, Inc., 2001.
- Dorman, Andy. "Internet Indiscretions." Network Magazine. June 2000. pp.100-104. Vol. 15, No. 6.
- "Encryption and Digital Signature Explained". Entrust. Canada, 1996.
- Golding, William. Lord of the Flies. New York: Coward-McCann, 1962.
- Government of Canada. Canada Customs and Revenue Agency. Strategy for Electronic Service Delivery. Ottawa: n.d.
- Government of Canada. Department of Foreign Affairs and International Trade. DFAIT Information Management Strategic Plan. Ottawa: July, 1999.
- Government of Canada. Electronic Commerce Branch of Industry Canada. Building Trust and Confidence in Electronic Commerce: A Framework for Electronic Authentication in Canada". Ottawa: 2000
- Government of Canada. Electronic Commerce Branch of Industry Canada. Canadian Internet Commerce Statistics Summary Sheet. August 22, 2000 <www.ic.gc.ca>.
- Government of Canada. Electronic Commerce Branch of Industry Canada. E-Com Fast Facts. May, 2000 <www.e-com.ic.gc.ca/english/fastfacts43d8.html>.
- Government of Canada. Electronic Commerce Task Force: Industry Canada. Electronic Authentication: Summary of Findings of Bilateral Consultations. Ottawa: October 1999.
- Government of Canada. Electronic Commerce Branch of Industry Canada. The Canadian Electronic Commerce Strategy. Ottawa: 1999.

- Government of Canada. Industry Canada. Connecting Canadians Information Kit. Ottawa: 2000.
- Government of Canada. Industry Canada and Department of Justice. The Protection of Personal Information: Building Canada's Information Economy and Society. Ottawa: 1998.
- Government of Canada. Statistics Canada. @Statcan: Special Issue 2001. Ottawa: 2001.
- Government of Canada. Statistics Canada. A Reality Check to Defining eCommerce. Ottawa: 1999.
- Government of Canada. Statistics Canada. Review of Statistics Canada Survey. July, 2000 <www.statcan.gc.ca>.
- Government of Canada. Statistics Canada. E-commerce and business use of the Internet The Daily, Ottawa: August 10, 2000. <www.statcan.gc.ca>
- Government of Canada. Parliament. Bill C-6: Personal Information Protection and Electronic Documents Act. Ottawa: August 7, 2000 <www.parl.gc.ca/36/2/parlbus/chamb.../bills/government/C-6_4/90052e>.
- Government of Canada. Parliament. Speech From the Throne. Ottawa: 1999. <www.parl.gc.ca>
- Government of Canada. Treasury Board of Canada Secretariat: CIO Branch. GOC PKI Initiative. Ottawa: 2000 <www.tbs.gc.ca>.
- Greenstein, Shane. "When Technologies Converge" IEEE Micro. January-February 1999. pp. 8-9. Vol.19, No. 1.
- Halsall, Fred. Data Communications, Computer Networks and Open Systems, Fourth Edition. United States: Addison-Wesley, 1995.
- Hontanon, Ramon. "Building a Robust Linux Security Solution." Network Magazine. March 1, 2000. Vol. 15, No. 3. <www.networkmagazine.com/article/>.
- Huxley, Aldous. Brave New World. New York: Harper and Row, 1965.
- "Internet Security Advice for Small and Midsize Enterprises". The Monthly Research Review. April 2000: pp. 16-17. GartnerGroup.
- King, Michael. "Mobile Security: Steps in the Right Direction". United States: Gartner, Inc., 2001.
- King, Michael, Delia MacMillan, Adam Sarner, Alexander Linden. "Wireless Web Data

- Services: Personalize or Perish". United States: Gartner, Inc., 2001.
- Kingwell, Mark. Dreams of Millennium. Toronto: Penguin, 1999.
- Klotz, Hattie. "Teen Girls Stage Their Own Web Revolution". Ottawa Citizen: Tuesday August 22, 2000 <www.ottawacitizen.com>.
- Knight, Stefan. "The Role of ADSL in Internet Access" Computer: July 1999, pp 9-10. Vol. 32, No. 7.
- Kroker, Arthur, Michael A. Weinstein. Data Trash. Montreal: New World Perspectives, 1994.
- Lawton, George. "Intellectual-Property Protection Opens Path for E-Commerce". Computer, Feb. 2000, pp. 14-21. Vol. 33, No. 2.
- Lessig, Lawrence. Code and Other Laws of Cyberspace. New York: Basic Books, 1999.
- Levine, Rick, Christopher Locke, Doc Searls, David Weinberger. The Cluetrain Manifesto. Cambridge: Perseus Books, 2000.
- Lukasik, Stephen J. "Will We Consider Ourselves Better Off?". IEEE Internet Computing. January-February 2000. pp. 47-49. Vol. 4, No. 1.
- Macedonia, Michael. "Why Digital Entertainment Drives the Need for Speed". Computer Magazine. February 2000. pp. 124-127.
- Malamud, Carl. "The Medium Should Not Be The Message". IEEE Internet Computing. January-February 2000. pp. 66-67. Vol. 4, No. 1.
- Menzies, Heather. Whose Brave New World? Toronto: Between the Lines, 1996.
- Metcalf, Bob. "The Next-Generation Internet". IEEE Internet Computing. January-February 2000. pp. 58-59. Vol. 4, No. 1.
- Milojicic, Dejan. et al. "Trend Wars: Internet Technology" IEEE Concurrency. January-March 2000. pp. 70-81. Vol. 8, No. 1.
- Mosco, Vincent. "Myth-ing Links: Power and Community on the Information Highway." E-Commerce vs. E-Commons: Communications in the Public Interest. eds. Marita Moll and Leslie Regan Shade. Ottawa: The Canadian Centre for Policy Alternatives, 2001. pp. 9-20.
- Reddick, Andrew, Christian Boucher and Manon Groseilliers. The Dual Digital Divide. Ottawa: The Public Interest Advocacy Centre, 2000.

- Riezenman, Michael J. "Technology 2000: Communications" IEEE Spectrum. January 2000. pp. 33-38. Vol. 37, No. 1.
- Richardson, Robert. "Public Key Infrastructure." Network Magazine. June 2000. pp. 114-120. Vol. 15, No. 6.
- Ruthowski, A.M. "An Internet Millenium Mosaic". IEEE Internet Computing. January-February 2000. pp. 44-77. Vol. 4, No. 1.
- Schiller, Dan. Digital Capitalism: Networking the Global Market System. Cambridge: MIT Press, 1999.
- Schrader, William L., and Chuck Davin. "Dissolution of the Old Order". IEEE Internet Computing. January-February 2000. pp. 64-65. Vol. 4, No. 1.
- Schwartz, Mike. "Mass Distribution of Ingenuity and Choice". IEEE Internet Computing. January-February 2000. pp. 68-69. Vol. 4, No. 1.
- Shapiro, Andrew L. The Control Revolution. New York: Public Affairs, 1999.
- Skvarla, Carol. "Broadband Wireless (MMDS/LMDS) in the U.S.: Perspective". United States: Gartner, Inc., 2001.
- Skvarla, Carol. "Wireless Technologies and Services: Overview". United States: Gartner, Inc., 2001.
- Smith, Carrie R. "Issues From the Networking Battlefield". The Monthly Research Review. April 1999: pp. 1-3. GartnerGroup.
- Steeves, Valerie. "Privacy Then and Now: Taking Stock Since IHAC." E-Commerce vs. E-Commons: Communications in the Public Interest. eds. Marital Moll and Leslie Regan Shade. Ottawa: The Canadian Centre for Policy Alternatives, 2001. pp. 49-56.
- Sterling, Bruce. "A Short History of the Internet". n.d.
<www.eff.org/pub/Publications/Bruce_Sterling/FSF_columns/fsf.05>
- Taylor, J. "Engineering in the Information Age". Engineering Management Journal. December 1998. pp. 277-287. Vol. 8 No. 6.
- "Technology's Inescapable Inabilities". The Monthly Research Review. March 2000: 1-2. GartnerGroup.
- The Internet and Beyond: Canadian Cable Industry". Canadian Cable Industry. March 2000. <www.ccta.com>.

Watchel, Bob. "All You Wanted to Know About T1 But Were Afraid to Ask". February 2001. <www.dcbnet.com/notes/9611t1.html>.

Wertheim, Margaret. The Pearly Gates of Cyberspace: a History of Space From Dante to the Internet. New York: W. W. Norton, 1999.

Willis David. "Nortel's Entrust". Network Computing. Nov. 1, 1996. <www.networkcomputing.com/717/717F1.html>.

Winseck, Dwayne. "Lost in Cyberspace." n.p. n.d. pp.1-19.