JIBC

Trust and Confidence and the Digital Economy: Issues and Challenges

Prabir K. Neogi and Arthur J. Cordell

Dr.Prabir K. Neogi(Electronic Commerce Branch, Industry Canada, 300 Slater Street, Ottawa, ON., Canada K1A 0C8,Email: neogi.prabir@ic.gc.ca) has a B.Eng. from Calcutta University in India and a Ph.D.(engineering) from London University (GB). After working for 9 years in the Computer Service Bureau Industry, he joined the Government of Canada in 1977. He worked for the Department of Communications and its successor, Industry Canada, where he is currently a Special Advisor with the Electronic Commerce Branch. His areas of work and interest include broadband infrastructure deployment and related networking issues, e-business adoption, digital divide issues and the socio-economic implications of the widespread adoption and use of information and communications technologies. He is particularly interested in the widespread adoption of General Purpose Technologies (steam, electricity, ICTs) and their transformative potential.

Dr. Arthur J. Cordell(Electronic Commerce Branch, Industry Canada, 300 Slater Street, Ottawa, ON., Canada K1A 0C8, Email: cordell.arthur@ic.gc.ca)received a BA from McGill University and a Ph.D.(economics) from Cornell University in Ithaca, New York. He has worked for the US Government in Washington and as a business consultant in New York. Arthur was a Science Advisor with the Science Council of Canada where he was closely associated with all Council studies on computers and communications. Arthur has also published widely in a number of academic and popular journals. Currently, Arthur Cordell is Special Advisor, Information Technology Policy, Industry Canada, Ottawa. His area of interest is the social, political and economic implications of information technology for Canadian society. He is co-author of such recent books as, *Shifting Time: Social Policy and the Future of Work (1994); The New Wealth of Nations: Taxing Cyberspace (1997)*. Both deal, in different ways, with the impact of information technology on the quantity and quality of work (the future of work and working); the productivity of networks and how that productivity may be more widely accessed and distributed; the promise and potential of electronic commerce.Arthur Cordell developed the idea of the 'bit tax', a way of getting at the productivity of a networked economy. The 'bit tax' also offers a way for different jurisdictions to apply a sales tax to electronic commerce. His current research is centred on the 'unintended consequences of information technology.'

Abstract

Globalization and technological change continue to profoundly affect economic growth and wealth creation. Information and Communications Technologies (ICTs) have been a key enabler and driver of globalization, which is likely to continue as trade and investment barriers continue to fall and communications become ever cheaper, easier and more functional. "National" economies, created by the Industrial Revolution in the 19th century, will continue to blend into a 21st century integrated, digital world economy, with an increasingly global division of labour.

Every economy requires a physical, institutional and legal infrastructure, as well as understandable and enforceable marketplace rules, in order to function smoothly. In this paper the authors maintain that such an infrastructure must be developed for the new digital economy and society, one which provides trust and confidence for all those who operate in or are affected

by it. An infrastructure that is an amalgam based on hardware, software, networks and a way of doing business which offers predictability, dispute resolution, legal recourse, policing powers against fraud,authentication, etc. The building of such an infrastructure is a necessary condition for the development and efficient functioning of a global, digital economy.

Introduction and Context

"The crime of identity theft undermines the basic trust on which our economy depends". President George W. Bush, as quoted by D. Scott Parsons, Deputy Assistant Secretary for Critical Infrastructure Protection, at the FDIC Identity Theft Symposium, Los Angeles, June 17, 2005 [29].

"Everything on the Web is ultimately about Trust." Nicholas Negroponte (http://www.blackhat.com/presentations/bh-usa-00/Edward-Schwartz/KellyandSchwartzPrivacy-1.ppt)

Globalization and technological change continue to drive economic growth and wealth creation. Over the last 25 years there has been a huge increase in global trade in goods and services, and global investment flows, and the pace of globalization is accelerating. Technology has been a key enabler and driver of globalization, which is likely to continue as trade and investment barriers continue to fall and communications become ever cheaper, easier and more functional. Today's "national" economies, created by the Industrial Revolution in the 19th century, will continue to blend into a 21st century integrated world economy, with an increasingly global division of labour for the production of both goods and services.

Global electronic networks of increasing power and pervasiveness form the communications backbone of this 21st century world economy, just as railroads, steamships, telegraphs and postal systems formed the transportation and communications infrastructure for the 19th century industrial economies. The foundation for the creation of the new digital economy, also referred to as the e-economy (the two terms will be used interchangeably) is the rapid and effective deployment of information and communication technologies (ICTs), in all sectors of the economy, and to consumers at large. Widely available, high powered networks allow information exchange at very low cost, reduce the negative role of distance and enormously increase the ability to coordinate geographically separated economic activities (cf. "The World is Flat" [5]). The central role of ICTs is increasingly identified as the fundamental factor in this economic transformation, which has also led to global supply chains [5] and the outsourcing and off-shoring of an increasing range of activities related to these supply chains. The commercial emergence of the ubiquitous Internet and the growing importance of electronic commerce and e-business in the global economy, are indicators of this transformation.

As noted above, the growth and productivity of advanced economies has relied heavily on ICT-based product and process innovation [18,22,23]. The key factor driving the implementation of e-business throughout the economy is the competitive advantage such technologies and applications offer to those who adopt them fully. E-business solutions allow organizations to streamline production, reduce operational costs, expand markets, increase revenues, enhance collaborative business partnerships and strengthen customer and supplier relationships [1]. By enabling collaborative activities to be carried out at widely dispersed locations, and by supporting process and product innovation through the application of e-business in all its various forms, networks have become an indispensable platform for industrial productivity and growth.

Firms as disparate as Wal-Mart and Dell Computers [5] represent outstanding examples of the use of ICTs to transform business processes and operations. Similarly, the use of computerized reservations systems has transformed the working of the huge travel and tourist industry. World-wide electronic credit authorization and payment systems, deployed by consortia such as VISA and MasterCard and firms such as American Express, have changed the way in which consumers shop and merchants do business.

Payments and financial transactions are the lifeblood of economies. Private sector joint ventures like Visa and MasterCard, along with the large banks, have helped to create a global electronic payments network. It is a dynamic, innovative system that spurs economic growth by providing fundamental benefits such as a safe, sound and predictable international payments network connecting buyers and sellers; ever-increasing levels of security and consumer empowerment; greater economic transparency; increased economic stimulation; and widened participation in the banking system. This global electronic payments network accrues benefits to economies and people around the world. The widespread adoption of electronic payments has significantly expanded the sales volume of goods and services, reduced the barriers to immediate credit and liquidity, and eased geographic restrictions to trade and exchange. To a growing extent, the Internet is playing a key role both as an enabler and as the infrastructure underpinning this transformation.

The Internet has become the central nervous system for the networked economy. As a global network of loosely connected Internet Protocol (IP) based networks, many thousands in number and growing rapidly, it reaches into every country in the world and provides businesses world-wide with a common platform for communication and commerce. In its various forms and functions, it has become an essential means of conducting and coordinating business activities across the economy as a whole, linking business supply chains continent-wide and globally, supplying and supporting financial services and creating a universal consumer marketplace.

Globally, the Internet is currently estimated to have almost 1 billion users [36], with very rapid growth occurring in developing countries like China and India. China alone is now estimated to have some 80 million Internet users. As in many other developed countries, most Canadians and virtually every business are now connected to the Internet. By 2004, some 82% of all firms in Canada, accounting for some 97% of Canada's gross business income, were connected to the Internet [25]. Consumers benefit from the added convenience these technologies and applications offer, including greater access to information and an expanded marketplace.

Since the Internet allows businesses to respond to consumers' inquiries, requests and transactions from any location, buying and selling online requires an international set of rules, where citizens, institutions and businesses can easily exchange information, products and services across borders and around the world with predictable results and protection. This makes conventional geographic borders less and less relevant. For example, personal information collected for an online purchase, by a company located in Vancouver from a Quebec-based consumer, could be stored on a server located in the United States or the Cayman Islands. As another illustration, information about the air travel movements of individuals who hold a membership in an airline loyalty program can be collected at a destination in Europe or Asia, and transferred back to Canada for inclusion in the program's database for later use.

The combined forces of technological change and globalization pose dramatic new challenges for public policy. In some respects, the Internet is similar to other ubiquitous communications networks that came before it. Just like the postal system, the telegraph and the telephone, we have come to rely on the Internet as an infrastructure that enables individuals and organizations to conduct commerce nationally and abroad, through the transmission of information. Like these other trusted networks, as we grow to depend on the Internet, a degree of safety and reliability is expected and needed.

But there is a key difference. Previous transportation and communications networks were birthed under the watchful eyes of regulatory or legislative bodies, at the national level or through international agreements. Users of such networks could have a modicum of confidence that their mail would not be tampered with, that railway lines would be inspected and maintained to ensure the safe running of trains, and that aircraft would take off and land at airports in an orderly manner through the operation of an internationally coordinated air traffic system. However, the Internet has evolved at an unprecedented rate and since it consists of an agglomeration of autonomous networks, it has characteristics quite unlike those of the earlier trusted networks. There are a number of potential challenges that must be considered if we are to benefit fully from its existence.

The Problematique

"?We will create a civilization of the Mind in Cyberspace". John Perry Barlow

"?you must recognize that the Internet was set up largely by academicians for limited use, but has grown beyond anyone's wildest expectations, with nearly one billion users today". Markus Kummer, Executive Coordinator, Secretariat WGIG [36].

"?The culture of the original Internet was one of trust". Leonard Kleinrock

The very success of the Internet as an economic tool and its ubiquity have lead to policy concerns and challenges revolving around the vulnerability of the network and the economic consequences of misuse.

The Internet started as the creation of a small group of dedicated researchers [12] and has now evolved into a widespread commercial information infrastructure, with tremendous influence on economies and societies. The Internet was never designed or intended for this kind of commercial use. When the Internet was designed in the 1970s, its designers did not expect that the network would have to be scaled to cover much of the world's population in over 180 countries, and security was not an important consideration. Concerns regarding security from hackers and phishers, congestion caused by spam, differentiated qualities of service, charging schemes and interconnection and revenue sharing arrangements between Internet Service Providers (ISPs) were not matters of major concern to the early designers and implementers of the Internet. These matters came to the fore as the Internet began to evolve into a ubiquitous commercial medium. *It is a profound challenge to retrofit these necessary features while the Internet continues to expand rapidly, and its proponents try to accelerate its adoption and use by increasing numbers of unsophisticated users.*

Networks like the Internet and its enabled services, such as electronic mail and web-based services, are inherently global in scope, operating across multiple jurisdictions to serve international clients and marketplaces. Their borderless nature creates the need to meet national policy goals through the design of new marketplace rules that can help to establish the trust and confidence required for doing business in this new environment. Over time, governments have played a crucial role by providing a positive legal and policy framework for technology innovation, investment and diffusion. As markets and technologies continue to evolve, the importance of a dynamic, responsive policy environment that provides clear and consistent ground rules for the conduct of electronic business will grow. The strengthening of business and consumer confidence in Internet applications and use, *especially measures to ensure a safe, secure and reliable Internet,* warrants particular attention from policy-makers.

Every economy requires a physical, institutional and legal infrastructure, as well as understandable and enforceable marketplace rules, in order to function smoothly. For national industrial economies, national and international infrastructures, as well as marketplace rules, were established through evolutionary processes that took many decades to reach fruition. The industrial economy achieved a stable institutional framework and communications infrastructure, built on national postal, telegraph and telephone systems, linked together by international institutions such as the International Postal Organization (IPO) and the International Telecommunications Union (ITU), to give them global reach. In a previous paper [18], the authors noted that a similar infrastructure must be created for the new economy. Such an infrastructure is based on networks (physical, institutional, legal) and a way of doing business which offers predictability, dispute resolution, legal recourse, policing powers against fraud, authentication, etc. In short, what is needed is an environment which provides trust and confidence for all those who operate, or are affected by the e-economy and society. *The authors further contend that it is useful to examine the structures and study the experience of these past successful systems, to see what lessons can be learned for the implementation of a robust cyber-infrastructure to serve the needs of a digital economy.*

This new infrastructure has been given many names; we have called it the cyber-infrastructure (CI) [18]. Parts are in place now, but more is needed. The authors contend that we must become more aware and knowledgeable about the need for a cyber-infrastructure, how it comes into being and how extensive it must be, to ensure the smooth functioning of global networks and the global digital economy they support. Only by understanding and acting on the need for a CI will markets function smoothly in a global, digital economy. An important related question is whether this can best be done by transforming the existing infrastructure and marketplace rules, or whether new institutional approaches and market mechanisms are required which are more fully congruent with the characteristics of the Internet and other global digital networks.

Public and Private Spaces

Much has been made of the uniqueness of the new world of information technology . It has been claimed that the cyber-infrastructure will be new and novel and unlike anything that has come before.

This is only partially true.*The technology is new but, as we have seen, the need for trust and confidence is similar to that which was developed in previous eras for earlier trustworthy infrastructures. There are other ways in which the cyber-infrastructure will have some characteristics that are quite familiar.*

Consider the issue of public space and private space.

In today's world we know that, for example, walking on a public sidewalk in any city carries with it certain protections and certain responsibilities. The pedestrian will cross at the crosswalk; cross on the green light; will try to be part of an orderly flow of other pedestrians; will not litter and will, in general, respect the rights of others. At the same time the pedestrian moves along with the knowledge that a variety of public authorities have ensured that the sidewalk is in reasonably good repair; that the law and police authorities offer protection; that there is legal protection regarding objects that might fall from buildings; legal protection vis-a-vis automobiles jumping the curb; protection from other motorized vehicles, etc.

Similarly, when the pedestrian moves into another space, a private space, the range of rules and responsibilities changes. The pedestrian might enter an office building, or a building that houses doctor's offices, or a shopping mall, or a hotel, or a bank. In each case there is a different set of "rules" that govern the protections and responsibilities that surround the pedestrian. Perhaps the pedestrian can only get to the desk or a security guard and must present a pass or can enter the shopping mall entirely or can enter the bank-only so far. To go further in the bank, say to the safety deposit boxes, further information must be provided to the bank authority.

On the other side it is commonly known, but rarely considered, that the pedestrian's rights have also changed as he/she moves seamlessly from public to private space. There is enhanced legal protection from panhandlers but diminished legal protections for "free speech." In the public space the pedestrian is free to go just about anywhere; in the private space the pedestrian's actions are circumscribed. In the public space a public law offers protection to the individual; in the private space there are private security guards and the public police are called usually only if a crime has been committed.

Or consider another familiar aspect of everyday life. We mail a letter or make a telephone call (especially on a landline) and can safely assume that there is no one listening in to the call and equally safely assume that letter has not been opened or read by others. In fact both actions are punishable by law.

By now the reader is probably asking: So what? What is new is that there is also a public space and a private space in the cyber-infrastructure. There is the public Internet -- a kind of sidewalk -- that is in the process of developing "rules of the road." And there are private spaces such as e-commerce sites, online banking, etc.

Over the many hundreds of years of law regarding public and private spaces, the rights and responsibilities of all parties have been well developed. They are so well understood that we don't give it a second thought as we move seamlessly from public to private and back to public space (finally moving to our own private space which is our home which offers its own set of protections and responsibilities.)

In the cyber world we are still in the process of delineating these boundaries and defining what happens when the boundaries are crossed and who is responsible for enforcement. When a bank is robbed it is clear where the enforcement takes place; when a keystroke spyware is secretly or covertly installed on a personal computer to record bank transactions and theft is later made from that account----who is responsible for enforcement? In the cyber world, citizens are constantly told to review their credit reports, their bank balances, etc., to make sure that their accounts have not been accessed and that their identities have not been stolen. We know that authorities are trying to stop such cyber crimes but the question is: which authorities? where? And how successful have been such authorities in stopping such cyber crimes and related activities?

Emails can be intercepted and read by employers, by hackers and by the individual's own internet service provider. It is a more open and less secure space. It seems to be a private communication but it is one that can be read by others and there seems to be no body of law that protects the integrity of the communication.

We are slowly getting used to the fact that the public space of the internet can be a "dark and dangerous" street with many unsavoury actors wanting to cheat us (with scams) or harass us (with spam) or otherwise grab our attention. Cyber citizens are traversing this public space with increasing care and some are deciding not to enter this public space at all (see below). Some are choosing not to go online, even to go to a secure private space. There is concern that the security of the private space in the cyber infrastructure does not bear the same resemblance to the security of the private space in industrial infrastructure. Online banking does not offer the same sort of trust and confidence as "bricks and mortar" banking. Online shopping, while convenient, means giving up credit card information to the uncertainty of cyber space. How certain is the shopper that the information has not been intercepted; that the web site is the "real" web site and not a replica created specifically by criminals?

We contend that a sustainable cyber infrastructure cannot be achieved on such a shaky foundation of trust, and that unless steps are taken to increase trust and confidence, then citizens are likely to eschew the "convenience" of the online world for the "inconvenience" but increased security of the offline world.

Living in a world of distrust is costly. This will hold true for the online world, as it held true earlier and holds true now for the offline world.

Going further to the home space of the cyber citizen, the home computer. We know that if a person's house is broken into, the police are called. It is a crime. But what if some spyware, in the form of unauthorized tracking software, has been unintentionally downloaded into the computer? Equivalent to a break in or to the crime of trespass, it is unclear who is responsible and how the criminal act will be addressed.

Can we reasonably expect that a secure cyber infrastructure can be run in a "wild west" fashion where each person is individually responsible? It seems unlikely. More likely is that we are still in an "institution building" period. A time when new institutional mechanisms in the public and private sectors will be created to deal with rights and responsibilities of public and private space in the cyber infrastructure.

Steps taken today and tomorrow by public and private actors will determine the characteristics of the online world. Perhaps the "dark and dangerous" public spaces will remain so and citizens will be willing to pay extra to enter a sort of "gated community" in cyber space. A private network with rules and regulations and methods of enforcement. Those who enter want and are willing to pay for the trust and security that they associated with the trust and security of the earlier infra-structure.

Or perhaps an international body (such as the International Postal Union) will be created to oversee the Internet and to provide rules of the road. Such a body would be one of member states who agree to enforce and prosecute offenders who violate the rules of the road.

What ever course is taken it is clear that leadership is needed. To do nothing is to turn the playing field over to the cyber pirates, thieves and extortionists. It is a council of despair and threatens to dramatically lessen the value of the Internet as a most valuable technology.

Issues and Challenges: Establishing an Environment of Trust and Confidence

". . commerce dies the moment, and is sick in the degree in which men cannot trust each other". Henry Ward Beecher (1813 - 1887) US clergyman, abolitionist In "Webster's Electronic Quotebase," ed. Keith Mohler, 1994.

The exchanges that take place between buyers and sellers of goods and services are the lifeblood of an economy, just as the exchanges that take place between citizens, their elected representatives and providers of public services are the lifeblood of a polity. For an economy or polity to work well, the parties to these different kinds of exchanges must trust each other and have confidence that the institutional framework within which they are operating is stable and that it will yield consistent, reliable and predictable results.

Countries around the world, as well as international bodies such as the OECD are all trying to develop a formula which will lead to an environment of trust and confidence in the electronic marketplace.

Canada has also developed a "shopping list" of what sorts of things are needed if trust and confidence is to prevail in the electronic marketplace.

We offer the following as illustrative of one country's approach.

One of the key objectives of Canada's Electronic Commerce Strategy [11] was to start the process of creating an environment of trust in which individuals and businesses would have as much confidence in the workings of the digital economy as they have in the workings of the traditional industrial economy. Creating this environment is a complex, evolving and ongoing challenge. Among other things, it involves measures to:

- authenticate and authorize parties to transactions;
- protect the privacy of personal information and the confidentiality of corporate information communicated or stored electronically;
- ensure that networks operate reliably;
- protect intellectual property rights in electronic goods and services, including developing the appropriate polices, practices and tools for digital rights management;
- establish a legal framework for contracts to function electronically;
- develop dispute resolution mechanisms that function effectively in an e-business environment; and
- protect individuals and businesses against annoying or abusive practices, such as unsolicited bulk e-mail (spam).

It is clear that the cyber-infrastructure that is put in place has to be one that carries with it, at a minimum, the same degree of trust and confidence as the current infrastructure (physical, legal, institutional) developed for the industrial economy.

Creating Trust and Confidence

To a large extent, the creation of an environment of trust and confidence involves the application of existing laws, regulations and commercial norms to the electronic environment, through the amendment or extension of existing instruments or through judicial interpretation. In some areas however, new instruments may be required. Given this context, made-in-Canada approaches should work in concert with general international cooperative initiatives.

Creating an environment of trust is not only the responsibility of policy-makers, regulators and the courts. As in any business environment, the private sector has a major role to play in its own right and in cooperation with government, in developing business norms, standards and codes of conduct, as well as in identifying and encouraging the adoption of best practices.

In sum, the task of building an environment of trust in the digital economy is complex. It involves actions to create an enabling legal and regulatory environment, to develop voluntary codes of practice, to educate businesses, consumers and public service providers and to create tools that are easy to use. This can only be done if all stakeholders work in partnership. What makes it particularly difficult is to try to do it in "Internet time", as opposed to the slow, organic way in which the previous infrastructure was developed [18]. Added to this, we are trying to retrofit a host of security features into an open system, the Internet, a system designed for convenience, research and ease of use. It is like building a community without locks anywhere and suddenly learning that locks on doors, on stores, on banks - locks and security are needed everywhere. Also that a retrofit is needed, as soon as possible, and that all players should "more or less" agree on the nature of the retrofit.

Spam and its Consequences

"Spam is more than a growing nuisance. It is a public policy issue that challenges governments, Internet Service Providers (ISPs), other network operators, commercial emailers and consumers to work together in new ways - with each stakeholder group fully playing its part - to solve a problem that threatens the interests of all." Report of the Task Force on Spam, May 2005 [6].

As examples of the types of the problems currently besetting the Internet, let us consider spam and its more virulent cousins like phishing, pharming and identity theft.

The problem of spam, or unsolicited commercial email, has become the Internet issue du jour because of its impact on email-enabled applications, which still constitute perhaps the most important use of the worldwide Internet. Some 11 billion emails were sent daily worldwide in 2001; this number grew to over 36 billion in 2004. Spam has been called a "growing cancer" on the body of the Internet; it has grown in volume to now place significant pressure on the Internet and its users. Spam is an intrusive nuisance to consumers; it costs businesses money in the form of lost worker productivity and their ability to market their products; and it harms Internet Service Providers (ISPs) and large corporate networks, because it uses up large amounts of bandwidth capacity and adds to technical support costs. These problems are worsening every day because the amount of spam is constantly rising. MessageLabs' estimates of the amount of spam as a percentage of all e-mail traffic have increased from 8% of US emails in 2001 to some 80% of all emails by the end of 2004, with a monthly average of 73%. Brightmail, a subsidiary of the leading Internet security firm Symantec, estimated that in June 2004 spam accounted for 65% of all Internet email. More recent estimates suggest that unsolicited, junk email on the Internet now represents some 80% of all emails sent [6]. *Spam has become a significant worldwide problem that clogs networks, consumes resources and, due to its implication in virus distribution, identity theft facilitation and other criminal activities, significantly erodes trust in electronic commerce.*

Estimates of the total cost of spam to the U.S. economy range from US$10 billion (Ferris Research) to US$87 billion (Nucleus Research). The Radicati Group and MessageLabs have estimated the worldwide cost of spam to businesses at US$20.5 billion in 2003. Other industry analysts estimate that the global cost of spam to businesses in 2005 will be around US $50 billion, in terms of lost productivity and increased network maintenance costs. Comparable figures for Canada are not readily available. However, it is clear that from the point of view of the spammer, this can be an extremely profitable business, with a relatively low cost of entry and rates of return that can be staggeringly high. This is why some have argued that *to effectively combat spam, one must significantly change the economics of spamming through a variety of coordinated measures, transforming it from the current profitable business model into a cost-prohibitive business model.*

The biggest potential cost of spam, however, is the loss of public confidence in Internet communications. At the macro level, spam is a direct threat to the viability of the Internet as an effective and trustworthy means of communication. By providing a vehicle for illegal activities like phishing and identity theft, as well as for the circulation of viruses and worms, spam undermines consumer confidence in e-commerce and electronic transactions between citizens and their governments. The atmosphere of distrust created by spam and its more virulent cousins imposes significant direct and indirect costs throughout the economy. Consequently, spam is also a direct threat to continuing economic prosperity, to more efficient public services and to the smooth functioning of a global, digital economy.

An analogy can be drawn to the start of the 20th century, when business practices were based on letters carried by the postal systems and telegrams for urgent communications. Signed letters and telegrams had standing in the courts of law. *If every three or even four letters and telegrams out of five had been fraudulent, could these business practices have continued?* A Pew Foundation study [4] shows that some 52% of Internet users consider spam a big problem and some 22% of email users have curtailed their use of email because of spam. Some businesses are considering abandoning the Internet altogether, in favour of private and closed user group networks, for operational and internal communications. Such networks could evolve to provide a premium tier of Internet access and services, with guaranteed security and quality of service, for those willing to pay, thus leading to a two-tier Internet. *Some have said that, if left unchecked, spam will bring the public Internet to its knees*.

Cyber-Crime: Phishing, Pharming and Identity Theft

"We can't go on business as usual, without risking the future of online commerce,?This is a watershed year. Everyone you talk to understands that their data aren't safe." Avivah Litan, Gartner Analyst [29].

"The story that needs to be told is the larger, long-term threat to the American financial industry. It's a cancer. It's not going to kill you now, but slowly, over time". Jim Melnick, Director of Threat Development at iDefense, quoted in the New York Times [27].

Identity theft is the criminal activity of assuming and using another individual's identity by wrongfully obtaining and using someone else's personal information, with a view to committing a forgery or a fraud for financial gain. Identity theft is facilitated by technology, and is a crime that takes a heavy emotional and financial toll on individuals as well as eroding consumer confidence.

In the age of the global Internet, identity theft is often associated with email "phishing", where emails which appear genuine are used to lure consumers to look-alike web sites with the names and logos of legitimate financial institutions, business and government agencies, for the purpose of stealing confidential information which can then be used for financial frauds. A nationwide US survey of 1,421 Internet users by the Pew Internet & American Life Project [4], conducted in January-February 2005, found that some 35% of email users had received unsolicited email requesting personal financial information. Phishers often contract with spammers to send out millions of increasingly sophisticated phony emails designed to lure victims to reveal personal and confidential information. A successful phishing operation could bring in thousands of fresh account numbers, along with other identifying details: names, addresses, phone numbers, passwords, PINs and mothers' maiden names. The richer the detail, the greater is the value and the better the selling price.

Similar in nature to email phishing, pharming seeks to obtain personal or private (usually financially related) information through domain spoofing. Rather than a consumer being spammed with malicious and mischievous email requests to visit spoof Web sites which appear legitimate, pharming 'poisons' a Domain Name Server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. The victim's browser, however will mistakenly show that he is at the correct Web site. This makes pharming much more serious and more difficult to detect. *Phishing attempts to scam people one at a time with an email, while pharming allows the scammers to target large groups of people at one time through domain spoofing.*

According to the U.S. Federal Trade Commission (FTC), identity theft is the fastest growing crime in North America that targets consumers [32]. In 2004, some 246,000 consumer complaints were filed to the FTC related to identity theft, and it was the fifth straight year that identity theft topped the list of consumer concerns. More recently *[27] the FTC estimates that about 10 million Americans have their personal information pilfered or misused in some way or another every year, costing consumers US$5 billion and businesses US$48 billion annually.*

PhoneBusters is an anti-fraud agency run by the Ontario Provincial Police (OPP), the Royal Canadian Mounted Police (RCMP) and the Competition Bureau, Canada. In 2003, 13,359 Canadians reported being victims of identity theft & direct losses totaled approximately $21 million. Statistics gathered by PhoneBusters in 2003 and the first half of 2004 indicate that the largest number of complaints surrounding identity theft relate to credit cards or to false applications for credit cards (32%) and cell phones and false applications for cell phones (10-12%).
(Source: Phonebusters,http://www.phonebusters.com/Eng/Statistics/idtheft_canada_stats_2003.html)[2].

The Canadian Council of Better Business Bureaus estimates that identity theft costs the Canadian economy approximately $2.5 billion (Cdn.) per year [1].

A February 2005 Ipsos-Reid poll [2] reported that some 9 per cent or 2.7 million Canadians have been victims of identity theft at some point over their lifetime. Ann Cavoukian, Ontario's Privacy Commissioner, observed recently that the crime had "exploded". She urged the Ontario provincial government to become the first in Canada to require private-sector firms to notify customers when files containing their personal information have been put at risk through loss or theft. In the US, the federal "Fair and Accurate Credit Transaction Act of 2003 (FACT Act)" [34] is intended to address this problem. Eight US states have introduced similar legislation, while another 30 states have bills pending [2,17].

Recently, there has been a spate of reports in the US about stolen credit card numbers and the existence of a thriving black market on the Internet in the trafficking of stolen credit card data. Thus the Washington Post [35] reported that according to MasterCard International Inc., more than 40 million credit card numbers belonging to US consumers might have been illegally accessed by a computer hacker and are at risk of being used for fraud. The breach occurred in late 2004 at a processing centre in Tucson, Arizona operated by CardSystems Solutions Inc., one of several companies that handle transfers of payment between the bank of a credit-card using consumer and the bank of the merchant where the purchase was made. While the banks which operate the Visa and MasterCard consortia are subject to regulation by appropriate authorities in different jurisdictions, the operations of 3rd party service providers like CardSystems Solutions are not subject to any similar regulation or public scrutiny. Their operations are only governed by their contractual agreements with the credit card companies. Officials at MasterCard and Visa have accused CardSystems of not meeting agreed-upon computer security standards, and Visa has suspended its contract with CardSystems.

The information that criminals siphon through phishing, pharming and similar activities - credit card and bank account numbers, as well as much raw consumer information such as Social Security numbers - is boldly bought and sold on the Internet through a thriving black market or Web bazaar. No one is willing to estimate how many cards and account numbers make it to the Internet auction block, but law enforcement agents describe the market as "huge". The value of the data arises from its ready conversion into online purchases, counterfeit card manufacture and more elaborate identity-theft schemes. Stolen credit card numbers allow thieves to make quick, fraudulent purchases. The losses have to be borne by the merchants, the credit card companies and ultimately the consumer.

A May 2005 survey of 5,000 U.S. online consumers by the Gartner Group, released on June 23, 2005 [29] contains a disturbing message for online retailers and bankers. More than 42% of online shoppers and 28% of people who bank online are cutting back on their activity because of "phishing" attacks and other assaults on sensitive data,.

About half of the US's 148 million Internet users believe they have received a phishing email, up 28% from a year ago, according to Gartner estimates based on its survey. Some 2.4 million online users have lost money to Internet scams, with total losses amounting to about $929 million in the 12 months ended in May 2005, Gartner estimates. According to the firm, Internet service providers and companies that serve consumers online now see 150 to 200 different phishing attacks each week, four times as many as they saw just six months ago.

More than 80% of those surveyed said concerns about Internet security have reduced their trust in email. Of these, more than 85% delete suspect mail without opening it, suggesting that some businesses sending legitimate email may be losing an efficient and low-cost method of communication with customers.

But the more obvious economic toll comes in consumers' increasing distrust of e-commerce and online banking. *According to the survey, 33% of online shoppers concerned with Internet fraud are spending less money than they would if they weren't concerned, and 77% of concerned online-banking customers said they are using online banking services less frequently. More than 4% of those Internet banking customers concerned with fraud have abandoned online banking altogether*.

In a recent article [27] the New York Times describes the workings of this Internet black market, through sites like http://iaaca.com),whose name is a shorthand for International Association for the Advancement of Criminal Activity (IAACA)! The online trade in credit card and bank account numbers, as well as raw consumer information is highly structured. There are buyers and sellers,intermediaries and even service industries. The players come from all over the world, but many of the web sites where they meet are run from servers located in the former Soviet Union, making them difficult to police. At a symposium on cyber-crime on May 2005 Jody Westby, the Managing Director of security and privacy practices at PricewaterhouseCoopers, claimed that based on FTC statistics and credit card theft, only about 5% of cyber-criminals are ever caught [27]."We are not making an impact?The criminals are too hard to track and trace, too hard to prosecute, and the information they steal is too easy to use". If this view proves to be correct over time, then *cyber-crime could become the Achilles heel of the global electronic payments system.*

Technological and Business Solutions: Tiered Networks?

"Expanding premium business services and offering customers new applications requires an infrastructure that removes the limitations of today's internet and that offers connectivity along with QoS (Quality of Service), reliability and security assurances. Underlying open standards will make the power of the IPsphere (the proposed premium networks) a reality."
Jochen Hagen |EVP, Product Management IP |T-Systems International
http://www.ipsphereforum.org/home

Although the Internet has changed all our lives, it was simply never built for commercial use. Discussions about the future of the Internet seem to go in one of two ways: how to make the existing network more secure; or, failing that, the inevitability of introducing a separate Internet---Internet Secure?--one which is closed, with security features built in from the beginning.

In this context, it is useful to distinguish between two broadly different classes of electronic networks: open networks and closed networks (see Annex 1). In Annex 1 we will also deal in more detail with the concept of an IPsphere, an IP-based public network that combines the ubiquitous connectivity of the Internet with the assured performance, reliability and security of a private network, and its proponent the IPsphere Forum.

Open networks, also referred to as public networks, have no restrictions on membership and are open to use by anyone willing to pay the established tariffs and abide by certain Acceptable Use Policies (AUP). They require the intervention of some sort of outside agency, usually a regulatory agency or policing function of government. This is to create and enforce standards and to regulate the behaviour of those using the network. The public Internet, a global network-of-networks consisting of over 50,000 loosely connected, IP-based networks spanning every country, is currently the best known example of an open network, but there are others which merit further study. One characteristic of the public Internet as it is presently run is that it has no well defined policing mechanism (a "they"), which can impose and administer sanctions for improper use such as spamming and phishing. In this sense the Internet differs from anything we currently know about in the "bricks and mortar" world. In every venue in our current world, there is a "they" that can step in if there is inappropriate or unlawful behaviour. In the Internet there is an absence of a "they".

Closed networks support the operation of a single entity (e.g. American Express, IBM, ATM networks dedicated to a single bank) or an existing closed user group, such as an association of financial institutions or airlines (e.g. SWIFT, Visa, MasterCard, SITA). Closed networks such as SWIFTnet or the Reuters currency trading network, which handle well over $1 trillion of financial transactions daily, are designed to provide and guaranty the necessary operational functionality, reliability and security for the members of the closed user group. There is a well defined policing mechanism (a "they") responsible for the design and operation, as well as overseeing the appropriate use of the network. Such networks are usually self enforcing, governments have a minimal or no role in their operation and the public is usually unaware of either the working of the network or when sanctions are administered because of transgressions.

One business model, which could provide a solution to many of the problems currently plaguing the public Internet, is a multi-tiered network. As stated earlier, some businesses are considering abandoning relying on the public Internet altogether, in favour of secure private and closed user group networks for operational and internal communications, with a secure gateway to the public Internet. The proponents of this concept claim that such networks could evolve to provide a premium tier of Internet access and services, with guaranteed security and quality of service, for those willing to pay. This would lead to a two-tier Internet. As long as the new premium blended nets are IP-based, controlled gateways between them and the public Internet could be designed with relative ease. This could be a logical business and technological solution. *Whether this is a desirable solution, from a public policy and welfare point of view, needs to be debated further.*

It should be noted that the current "bricks and mortar" world consists of a broad and near infinite range of security for businesses and consumers, customized for various needs. From open commerce on the sidewalks to the security of the bank, there is a range of ways of buying and selling that carry more or less security and carry more or less cost to ensure that security. We may well be on the verge of witnessing a similar development in cyber-space. This would result in a range of security enabled services, with protections customized to the requirements of applications and paid for by various interested parties throughout the networks.

IPspheres, earlier referred to as infranets [21], are IP-based networks that combine the reach of the Internet with the assured performance and security of a private network. They provide another variant of the multi-tiered Internet business model, which is supported by a number of major service providers (see Annex 1). The IPsphere Forum, which formally came into existence on June 28, 2005, is an initiative of industry leaders focused on driving the development and implementation of IPspheres. This new approach is designed to overcome the current limitations of the Internet, delivering an enriched experience for consumers, business-critical performance, and opening new markets for service providers. It is expected that ultimately service providers will connect IPspheres together to create a single, global meta-network capable of carrying ALL communications. However, the IPsphere concept is still in its infancy, and a migration path from the current public Internet to an IPsphere world would still have to be established and implemented.

The Role of Governments

"To say that governments and their law enforcers should stay out of cyberspace is as naive as saying they should stay out of city centres ... The Internet may be the cleverest infrastructure the world has ever known, but it is not a world apart." Editorial in the New Scientist, May 8, 1999. [18]

"... Similarly, Government cannot simply regulate to achieve its aims in this new global economic environment. This Report, therefore, recommends a light regulatory touch. Enough to build confidence in the new way of doing business and to protect consumers, but not so much that we stifle innovation,

creativity and entrepreneurship and drive industry overseas." Prime Minister Tony Blair, Foreword to the UK Cabinet Office report ecommerce@its.best.uk , September 1999 [30].

Driven by the economic importance of networks and information technology, many governments are reviewing their policy frameworks in areas as diverse as telecommunications policy, competition law, Internet policies, intellectual property law and media regulation, broadband networking strategies, security and public safety, and spectrum regulation. The trend seems to be a movement toward frameworks that establish broad ground rules for investment in modern networks and encourage network use within a competitive market environment, optimising their application across technologies, industries and jurisdictional boundaries.

The historical role of governments in ensuring the orderly implementation of broad, general purpose technologies which are enabling and transformative in nature, is well-known. One need only consider the extensive frameworks of legislation and ways of behaving that surround railroads, electricity, the telephone and the automobile.*For the Internet to achieve its maximum social and political potential there will have to agreed upon and effective rules of the road, both nationally and globally*

Government can play a critical role in developing and determining marketplace rules for the digital economy. Such rules can affect the pace of ICT based innovation as well as provide the foundation for the development of a high level of trust and confidence which is necessary for the successful operation of electronic marketplaces. Data protection and privacy, electronic signatures and authentication, spam and cyber-crime, including the threat of identity theft, have emerged as important areas where governments need to be either directly or indirectly involved in establishing such rules of the road.

The Canadian government has played a significant role in fostering the development of network infrastructure for today's information economy, as well as the ground rules that will be needed for an increasingly network-based economy. Such rules must not only adapt to new technologies, but also reflect the global, borderless nature of modern trade and commerce. Future economic growth, moreover, relies on a set of rules which are consistent and apply marketplace-wide. Accordingly, in order to maintain Canada's competitive position internationally, the government has acted to make Canada a world leader in the adoption and use of electronic commerce, by creating a predictable and supportive environment that would ensure consumers and businesses feel comfortable, secure and confident in conducting commerce online.

Traditional policy and regulatory instruments are usually limited in their application to national or sub-national jurisdictions. In the absence of complementary actions in other jurisdictions, however, domestic rule-making for marketplaces which are defined by the conduct of Internet-based business, will have limited effectiveness. Thus, in order to meet national policy objectives effectively in areas such as data protection and privacy, electronic signatures, the regulation of spam and other offensive Internet content, and consumer protection measures, governments need to coordinate and align their domestic regimes with those in force outside their own jurisdictions, both bilaterally and on a multilateral basis.

The public policy challenge for governments rests on their ability to redesign the ground rules for the conduct of international business - first, by adapting the traditional trade rules and disciplines developed through bodies such as the World Trade Organization (WTO) and in regional agreements such as the FTAA, to the realities of a networked international economy dominated by e-business, and secondly, to harmonize the operation of domestic legal, policy and regulatory frameworks with international norms.

The UN Working Group on Internet Governance (WGIG) has recently released a Report [36] which will be considered at the World Summit on the Information Society (WSIS) meeting in Tunis in November 2005. The document makes recommendations in a number of policy areas related to Internet governance such as: administration of the root zone files and system; allocation of domain names; IP addressing; interconnection costs and multi-lingualism. There are also recommendations relating to Internet stability, security and cyber-crime; spam or junk emails; data protection and privacy rights; consumer rights; intellectual property rights; freedom of expression; capacity building and meaningful participation in global policy development. The WGIG report lays out four possible models for the conduct of global public policy and oversight of the Internet. Further developments are expected at the WSIS meeting in November 2005.

Spam is currently the subject of legislative and regulatory action in the U.S. [33], Europe and other jurisdictions. It is an example of emerging issues which warrant rapid, flexible approaches from public policy-makers. Rather than traditional regulatory approaches, Internet economy issues like spam require concerted action by governments and the private sector aimed at establishing practical rules of the game, and cooperative enforcement. Business practices to protect customer information and prevent the theft of identification data are key to meeting growing security problems. But business and consumer action is only one part of the solution. Governments must also take the necessary legislative steps to effectively address these issues, including amending and strengthening existing legislation as necessary and working closely with businesses and consumers. In Canada the Ministerial Task Force on Spam, in its report [6] to the Minister of Industry, has proposed a multi-faceted strategy for combating spam. The implementation of its Recommendations will require a coordinated and concerted approach among all stakeholders.

So serious is the threat of spam and cyber-crime that cooperative, multi-jurisdictional enforcement of civil and criminal sanctions will most likely be required to stem the tide. Ideally, due to the borderless nature of electronic markets and services, such marketplace rules should work both domestically and across international boundaries and thus facilitate the seamless flow of commerce across a networked business environment. The economic interdependence resulting from globalization and the increasing prominence of information and communications technologies in trade and commerce has magnified the importance of having international legal, policy and regulatory ground rules which govern the working of the global information economy.

Key Findings and Conclusions

The combined forces of technological change and globalization pose dramatic new challenges for public policy. The widespread deployment and use of the Internet by businesses and consumers has lead to the emergence of a borderless, international marketplace which operates across multiple borders and legal jurisdictions. While a major factor in stimulating productivity and economic growth, the emergence of an Internet-based global economy poses important new challenges for governments everywhere. In the first instance, a network-driven economy raises new policy concerns in areas like network access and availability, as well as the protection and security of information. Secondly, to reach its full economic potential, the networked economy relies on establishing a complete set of consistent ground rules for the conduct of electronic trade and commerce that will apply seamlessly across the entire marketplace, not only within but also between territories and jurisdictions.

In some respects, the Internet is similar to other ubiquitous and trusted communications networks of the industrial era that came before it. But there is a key difference. Previous transportation and communications networks were birthed under the watchful eyes of regulatory or legislative bodies, at the national level or through international agreements. The Internet has evolved at an unprecedented rate and it consists of an agglomeration of autonomous and apparently self-regulating networks. However, there is no gatekeeper or "watchdog" person or agency to oversee activities on the Internet: a "they" that can step in when governance or "policing" is necessary to curb inappropriate or criminal use. It is a profound challenge to retrofit this necessary functionality while the Internet continues to expand rapidly and its proponents try to accelerate its adoption and use by increasing numbers of unsophisticated users.

Although the Internet has changed all our lives, it was simply never designed and built for ubiquitous and global commercial use. While the technology is new, the need for trust and confidence carries over from an earlier era. A sustainable cyber infrastructure cannot be achieved on a shaky foundation of trust, and unless steps are taken to increase trust and confidence, then citizens are likely to eschew the "convenience" of the online Internet world for the "inconvenience" but increased security of the offline world and the private networks.

Spam has become a significant worldwide problem that clogs networks, consumes resources and, due to its implication in virus distribution, identity theft facilitation and other criminal activities, significantly erodes trust in electronic commerce. If left unchecked, spam will bring the public Internet to its knees. Cyber-crime, Internet fraud and identity theft are likely to become even more serious problems. Cyber-crime could become the Achilles heel of the global electronic payments system.

Living in a world of distrust is costly. This will hold true for the online world, as it held true earlier and holds true now for the offline "bricks and mortar" world. It is clear that the cyber-infrastructure that is put in place has to be one that carries with it, at a minimum, the same degree of trust and confidence as the current infrastructure (physical, legal, institutional) developed for the industrial economy. The task of building an environment of trust in the digital economy is complex. It involves concerted actions among many stakeholders: to create the requisite legal and regulatory environment; to develop voluntary codes of practice; to educate businesses, consumers and public service providers; and to create tools that are easy to use.

For the Internet to achieve its maximum social and political potential there will have to be agreed upon and effective rules of the road , both nationally and globally. This new technology will have its own unique regulatory framework, but it will only flourish if there is some early agreement and acceptance of both broad and specific governance approaches aimed at buttressing the vital areas of trust and confidence.

Acknowledgements

The authors wish to thank Mr. Don MacLean, a colleague and close friend, the author of the Industry Canada Discussion Paper "The Challenge of Change: Building the 21st Century Economy" and the Report of the Ministerial Task Force on Spam "Stopping Spam: Creating a Stronger, Safer Internet". They also wish to thank Mr. Richard Simpson, the Director-General of the Electronic Commerce Branch. It goes without saying that any views expressed in our paper are those of the authors, and do not necessarily represent the views of Industry Canada, or the Government of Canada.

A version of this paper was initially prepared for the 2005 Networking and Electronic Commerce Research Conference (NAEC 2005), held at Riva del Garda, Italy October 6-9, 2005 http://atsma.org/NAEC2005/

References

(1)Canadian e-Business Initiative(CeBI): "Fast Forward 4.0: Broadening Canada's Digital Economy", May 2003."Fast Forward 5.0: Growing Canada's Digital Economy", September 2004. Available at http://www.cebi.ca

(2)Consumer Measures Committee(2005): "Working Together to Prevent Identity Theft: A Discussion Paper" Discussion Paper released July 6, 2005 by the Consumer Measures Committee as part of the Identity Theft public consultation. Available at http://www.cmcweb.ca/idtheft/

(3)Cordell, A.J., Ide, T.Ran, Soete, L. and Kamp, K. (1997): "The New Wealth of Nations: Taxing Cyberspace",Between The Lines, Toronto, Canada.

(4)Fallows, Deborah(2003): "Spam: How it is Hurting Email and Degrading Life on the Internet", Report of the Pew Internet & American Life Project, October 22, 2003. From the same author and source see also the Data Memo "CAN-SPAM a year later", April 2005. Available at http://www.cmcweb.ca/idtheft/

(5)Friedman, Thomas L. (2005): "The World is Flat: A Brief History of the 21st Century", 1st. ed., Farrar, Strauss and Giroux, New York, 2005. ISBN-13: 978-0-374-29288-1.

(6)Industry Canada(2005): "Stopping Spam: Creating a Stronger, Safer Internet", Report of the Ministerial Task Force on Spam, May 2005. Available at hhttp://www.e-com.ic.gc.ca. See also the Task Force Reports and Publications available separately.

(7)Industry Canada(2004): "The Challenge of Change: Building the 21st Century Economy", Background Paper prepared for the Conference "e-Commerce to the e-Economy: Strategies for the 21st Century", Ottawa, September 27-28, 2004. Available at http://e-economy.ca

(8)Industry Canada(2004): "Principles for Electronic Authentication - A Canadian Framework", May 10, 2004. Available at http://www.e-com.ic.gc.ca

(9)Industry Canada(2004): Ministerial Task Force on Spam: News Release and Backgrounder, May 11, 2004. Available at http://www.e-com.ic.gc.ca

(10)Industry Canada(2003): "E-mail marketing: Consumer Choices and business opportunities", Discussion Paper, Ottawa, January 2003. Available at http://www.e-com.ic.gc.ca

(11)Industry Canada(1998): "The Canadian Electronic Commerce Strategy", Ottawa, September 1998.

Available at http://www.e-com.ic.gc.ca

(12)Internet Society: "A Brief History of the Internet", Available at http://www.isoc.org/internet/history/brief.shtml

(13)Internet News(2004): "Record Broken: 82% of US Email is Spam", May 5, 2004. Available at www.internetnews.com/stats/article.php/3349921

(14)Internet News(2004): "The Cost of Phishing Hits $1.2 Billion", May 6, 2004. Available at http://www.internetnews.com/ec-news/print.php/3350891

(15)Ipsos-Reid(2003): "Concern about Identity Theft Growing in Canada", February 28, 2003.

(16)Lessig, Lawerence(2000): "Code and Other Laws of Cyberspace", Basic Books, 2000.

(17)McAfee(2005): "McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet", available at http://www.mcafeesecurity.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf

(18)Neogi, P.K., Cordell, A.J.(2004): " Cyber-infrastructure and the Digital Economy: Managing the Transition", paper presented to the 7th International Conference on Electronic Commerce Research, Dallas, June 10-13, 2004.

(19)Neogi, P.K., Leduc, A., Peters, C.(2003): "Internet Connectivity and E-Business Adoption by Canadian Firms: An Empirical Analysis", paper presented to the 6th International Conference on Electronic Commerce Research, Dallas, October 23-26, 2003.

(20)Network World Canada(2005): "Introducing the infranet", January 7, 2005. Available at http://www.ITworldcanada.com

(21)Nolle, Thomas(2004): "Infranets: Fulfilling IP's Promise", CIMI White Paper, available at http://www.ipsphereforum.org/

(22)OECD (2004): "The Economic Impact of ICT: Measurement, Evidence and Implications", Paris, 2004.

(23)OECD (2003): ASeizing the Benefits of ICT in a Digital Economy@, Paris, 2003.

(24)Simpson, R., Neogi, P.K., Leduc, A., Peters, C.(2001): "The New Networked Economy: Trends, Challenges and Opportunities", paper presented to the 4th International Conference on Electronic Commerce Research, Dallas, November 8-11, 2001.

(25)Statistics Canada "Survey of Electronic Commerce and Technology" 2000, 2001, 2002, 2003, 2004. "The Daily", Catalogue No. 11-001-XIE.Available at http://www.statcan.ca

(26)The Economist (2004): "Make 'em Pay: The dismal science takes on spam", February 12, 2004.

(27)The New York Times(2005): "Black Market in Stolen Credit Card Data Thrives on Internet", June 21, 2005.

(28)The New York Times(2005): "Law Barring Junk E-Mail Allows a Flood Instead", February 1, 2005.

(29)The Wall Street Journal(2005): "Internet Scams, Breaches Drive Buyers off the Web, Survey Finds" , June 23, 2005.

(30) UK Cabinet Office report "ecommerce@its.best.uk" , September 1999.

(31)U.S. Department of Commerce(2003): Economics and Statistics Administration "Digital Economy 2003", Washington, December 2003.Available at http://www.doc.gov

(32)US Federal Trade Commission(2002): Submission to the Senate Judiciary Committee's Sub-committee on Technology, Terrorism and Government Information, March 20, 2002.

(33)U.S. legislation(2003): "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003)".

(34)U.S. legislation(2003): "Fair and Accurate Credit Transactions Act of 2003 (FACTA 2003)".

(35)Washington Post(2005): "40 Million Credit Card Numbers Hacked", June 18, 2005.

(36)WSIS WGIG(2005): "Report of the Working Group on Internet Governance", released July 14, 2005. Available at http: www.wgig.org/

Annex 1: Closed and Open Networks

In the context of electronic packet-switched networks, it is useful to distinguish between two broadly different classes of networks: closed networks and open networks.

Closed networks support the operation of a single entity (e.g. American Express, IBM, ATM networks dedicated to a single bank) or an existing closed user group, such as an association of financial institutions or airlines (e.g. SWIFT, Visa, MasterCard, SITA). Closed networks such as SWIFTnet or the Reuters currency trading network, which handle well over US$1 trillion of financial transactions daily, are designed to provide and guaranty the necessary operational functionality, reliability and security for the members of the closed user group. There is a well defined "they" responsible for the design and operation, as well as policing the appropriate use of the network. Such networks are usually self enforcing, governments have a minimal or no role in their operation and the public is usually unaware of either the working of the network or when sanctions are administered because of transgressions. Many such private or closed user group networks are now converting, or have already converted to the IP standards, while maintaining or even enhancing the necessary operational functionality, reliability and security.

SWIFT (Society for Worldwide Interbank Financial Telecommunication - http://www.swift.com is the financial industry-owned cooperative supplying secure, standardised messaging services and interface software to some 7650 financial institutions in over 200 countries. SWIFT's worldwide community includes banks, brokers/dealers and investment managers, as well as their market infrastructures in payments, securities, treasury and trade. SWIFT has been in operation for over 30 years and the network has evolved continuously, to take advantage of technological advances. SWIFTnet, the cooperative's new IP-based messaging platform, is being rolled out.

The Visa and MasterCard networks are perhaps the largest and most widespread examples of such global, cooperative networks. Visa, the world's leading payment brand with unsurpassed acceptance in over 150 countries, generates more than US$2.5 trillion in annual card sales volume. Every card issuing financial institution and every merchant with a Visa or MasterCard account, requires access to these networks for carrying out an electronic, credit authorization transaction. Private sector joint ventures like Visa and MasterCard have helped to create a global electronic payments network. It is a dynamic, innovative system that spurs economic growth by providing fundamental benefits such as a safe, sound and predictable international payments network connecting buyers and sellers; ever-increasing levels of security and consumer empowerment; greater economic transparency; increased economic stimulation; and widened participation in the banking system. This global electronic payments network accrues benefits to economies and people around the world.

Open networks, also referred to as ***public networks,*** have no restrictions on membership and are open to use by anyone willing to pay the established tariffs and abide by certain Acceptable Use Policies (AUP). They require the intervention of some sort of outside agency, which can be a voluntary body but more usually is a regulatory agency or policing function of government. This is to create and enforce standards and to regulate the behaviour of those using the network. The public Internet, a global "network-of-networks" consisting of over 50,000 loosely connected, IP-based networks spanning every country, is currently the best known example of an open network, but there are others which merit further study. One characteristic of the public Internet is that, since it consists of thousands of autonomous networks spanning a large number of jurisdictions, it has no well defined "they", i.e. a national or international agency or body which can impose and administer sanctions for improper use such as spamming, phishing and pharming. By default, such a role tends to fall on the major Internet Service Providers (ISPs), but it is not clear whether a consortium of the major ISPs would have either the financial incentive or even the power to "police" the public Internet.

The IPsphere: the Path to the Future?

Although the Internet has changed all our lives, it was simply never built for commercial use. It can only function in two dimensions: connectivity and bandwidth.

An IPsphere, formerly referred to as an "infranet", (http://www.ipsphereforum.org/)is an IP-based public network that combines the ubiquitous connectivity of the Internet with the assured performance, reliability and security of a private network. Conceptually, IPspheres will offer assurances in multiple dimensions: quality, reliability and security without compromising the connectivity and bandwidth dimensions.

When implemented, IPspheres will provide important benefits across the service delivery value 3 chain.

- IPspheres will enable any customer application to automatically request the level of security, quality and bandwidth it requires from the network.
- IPspheres will provide dynamic assurances - delivering services with the level of performance and security required by each customer application.
- IPspheres will support and reward the extension of advanced services, such as content distribution and high performance virtual private networks, across the global public network - well beyond the confines of one physical network.

The IPsphere Forum, which formally came into existence on June 28, 2005, is a team of industry leaders focused on driving the development and implementation of IPspheres. This organization is comprised of technology leaders from across the industry, including network service providers, network equipment vendors, and application and software vendors. Members include America Online, Alcatel, British Telecom, Cisco, Ericsson, France Telecom, HP, IBM, Juniper Networks, Lucent Technologies, Microsoft (?), Oracle, Qwest, Siemens, Tellabs, Telstra and Time Warner Telecom. The Forum will set the priorities for, and oversee the progress of, working groups involved with the d evelopment and definition of new technologies that will enable IPspheres to be successfully architected and implemented.

The goal of the IPsphere Forum is to create an industry call to action to create public networks that combine the reach of the Internet with the assured performance and security of a private network. This new approach is designed to overcome the current limitations of the Internet through the creation of "IPspheres," delivering an enriched experience for consumers, business-critical performance, and opening new markets for service providers. IPspheres are still in their infancy. However, it is expected that ultimately service providers will connect IPspheres together to create a single, global meta-network capable of carrying ALL communications.

The service provider industry does have a choice. It can collaborate to address the challenges identified in the IPsphere vision, or it can continue down the path of multiple, disparate, application-specific public networks. It's increasingly clear that the first of these choices is the most economically viable.

The IPsphere approach also has a very strong precedent - the Public Switched Telephone Network (PSTN). The sustained economic success of the PSTN demonstrates the power of industry collaboration on a single set of standards. The PSTN also demonstrates how a network that combines global, any-to-any connectivity and performance assurances can enable a diversity of follow-on, unanticipated applications and services. For example, without the PSTN and the dial-up services it enables, the Internet would likely have remained a research and education tool.

If IPspheres, or something like them, do not come to fruition, we will continue to experience the economic consequences of multiple, disparate approaches to network services.