Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, August 2010, vol. 15, no.2
(*http://www.arraydev.com/commerce/jibc/*)

The Internet and the Need for Governance: Learning from the Past, Coping with the Future

Dr. Prabir K. Neogi
Special Advisor, Electronic Commerce Branch, Spectrum, Information Technologies and Telecommunications Sector, Department of Industry, Government of Canada
Postal Address: **Jean Edmonds Tower North, R 1854C, 300 Slater Street, Ottawa, ON, Canada K1A 0C8**
Email: ***prabir.neogi@ic.gc.ca***

Dr. Prabir K. Neogi has a B. Eng. from Calcutta University (India) and a Ph.D. (engineering) from London University (GB). His areas of interest include broadband infrastructure deployment, e-business adoption, digital divide issues and the socio-economic implications of the widespread adoption and use of information and communications technologies. Particularly interested in the widespread adoption of General Purpose Technologies (steam, electricity, ICTs) and their enabling and transformative impacts.

Arthur J. Cordell, Ph.D.
Adjunct Professor, Carleton University, School of Mass Communications
Postal Address: **346 St. Patrick's Building, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6**
Email: ***Denart40@sympatico.ca***

Dr. Arthur J. Cordell 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 City. He was a Science Advisor with the Science Council of Canada. Recently, Arthur Cordell retired from his position as Special Advisor, Information Technology Policy, Industry Canada, Ottawa. He is currently an Adjunct Professor at Carleton University.

Abstract

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 the building of such an infrastructure, which provides trust and confidence for all those who operate in or are affected by it, is a necessary condition for the development and efficient functioning of a global, digital economy. They also show that costs will result if the global economy has to function on the basis of distrust, both at the individual and transaction level.

Although the Internet has transformed the economy, society and politics, it was never designed and built for global, ubiquitous and secure commercial use. While the technology is new, the need for trust, confidence and security remains. The Internet is an open network where there is no outside body that can administer sanctions. In this respect, it appears to be unique in commercial history. One characteristic of the public Internet is that, since it consists of many thousands of autonomous networks spanning a large number of jurisdictions, it has no well defined oversight mechanism that can administer sanctions. Drawing upon the lessons of history and historical analogies, the authors indicate some possible solutions. 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.

Keywords: **Internet; Trust; Governance; Oversight**

INTRODUCTION AND CONTEXT

> "…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.

> "Trust is the spinal cord of economics".
> From keynote remarks by **Angel Gurría**, OECD Secretary-General, delivered at 2009 BIAC Business Roundtable, May 2009, Lisbon, Portugal

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.

THE ENABLERS AND DRIVERS OF GLOBALIZATION

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 creation of the new digital economy is based on the rapid and effective deployment of information and communication technologies (ICT's), in all sectors of the economy, and to consumers at large. Widely available, high capacity 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. Recent developments like "Cloud Computing" simply reinforce these ongoing and well established trends [18].

The central role of ICTs is increasingly identified as the fundamental factor in this economic transformation, which has also led to global supply chains [2] 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. To a growing extent, the Internet is playing a key role both as an enabler and as *the* infrastructure underpinning this transformation.

THE ROLE OF THE INTERNET

> *"…the Internet has become the major platform for global commerce -- the equivalent of the shipping lanes that facilitated world trade in the days of Magellan or the railroads that opened the west during the Industrial Revolution".*
> Ivan G. Seidenberg, Chairman of the Board and Chief Executive Officer of Verizon, Speech to the Council on Foreign Relations, New York, April 6, 2010.

The Internet has become the central nervous system for the digital economy. As a global network of autonomous, 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.

The Internet is inherently global in its scope and nature. 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. 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.

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 digital economy raises new policy concerns in areas such as network access and availability, as well as the protection and security of information. Secondly, to reach its full economic potential, the networked economy will need 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.

Because businesses and consumers have grown to depend on the Internet, its uninterrupted and reliable operation is both needed and expected. However, online security threats have increased and the degree of trust and confidence in the Internet as a safe and reliable environment for electronic commerce is being negatively affected. Some of these threats, such as phishing and spyware, target Canadians who use the Internet for online banking and e-commerce. Other threats, such as spam and botnets, have the potential to affect everyone who uses the Internet for e-mail and web browsing. Canadians are well aware of these threats. The 2007 Canadian Internet Use Survey [21] estimated that 50% of Canadians were very concerned about online credit card use, 44% about online banking transactions, and 37% about the protection of their privacy online.

THE PROBLEMATIQUE: THE NEED FOR GOVERNANCE

> "…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 of the Secretariat, Working Group on Internet Governance (WGIG), 2005. [25].

> "…Given that this infrastructure has become critical to our economies and societies, we should all engage in developing better, more broad-based, governance arrangements and policies".
> OECD Secretary-General Angel Gurría, in the closing session of the OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, June 17-18, 2008. [19]

In the early days of the Internet (before the name Internet was even coined), its development and use was characterized by a small group of academics and researchers who knew each other and formed a community of interest. As in any typical small community, behaviour on the early net was self-regulating. While a small town needs a sheriff as final law officer, the closeness of inhabitants means that people will usually behave in ways that seek to avoid shame for themselves and their families. As communities grow there is a concomitant growth in anonymity. Anonymity allows for behaviour that might be unthinkable in a small community. The old adage "change in quantity leads to a change in quality" applies to communities and applies to the net as

well. When the net was a small group, self-regulation was adequate. When a community is small it too is largely self-regulating. When the community grows to a large city there is a need for both regulation and enforcement. There is also a need for oversight and sanctions, where needed.

As the Internet has grown and become a vehicle for business applications and e-commerce, a fundamental problem has been revealed: it is virtually impossible to regulate or enforce the behaviour of the net-citizens. With all previous networks there has been an enforcement mechanism to provide sanctions when misbehaviour or outright criminal activities take place. In the world created by the automobile, society learned early on that both the drivers and their vehicles needed to be licensed, and rules of the road created and enforced for public safety and security. Enforcement and sanctions were and are done by a particular designated and authorized entity. We refer to these entities as the “Theys”. In most aspects of our lives there is a “they” that can intervene if rules, written or unwritten, are breached. Network after network (rail, airlines, telecommunications, broadcasting, etc.) all have a "they", as in: "if you break the law, they will...(take away your license, send you to jail, issue a fine, etc.).

With the Internet we are presented with a wholly unique situation, which is described further in the next section. Society has ramped up a small research network into a global network of networks with more than 1 billion users in some 200 countries. The Internet is increasingly critical to national and global economic well-being, and there is no “They”: there is no effective mechanism for regulation or enforcement. This is only one of a number of potential challenges that must be considered if we are to benefit fully from its existence.

A LESSON FROM HISTORY

A physical, institutional and legal infrastructure, as well as an understandable and enforceable set of marketplace rules, are needed by all economies if they are to function smoothly. This has been true from the earliest pre-industrial days when commerce was marked by the barter of goods and services, and continued through the industrial “bricks and mortar” era. While many say that “the Internet changes everything” we contend that one thing remains unchanged: an Internet economy or the “new economy” will also require understandable and enforceable marketplace rules.

From the earliest beginnings of trade and exchange, in the civilizations of Egypt, Sumeria, the Indus valley and China, there was the need for some sort of understandable, predictable and respected infrastructure.

In earlier times the physical, legal and institutional infrastructure was probably bound up in a family, or a tribe. The patriarch or leader encapsulated these aspects. As the micro economy developed to include other families and other tribes, so too did the infrastructure develop in ways that trade and exchange could take place within an atmosphere of trust and confidence.

This is not to say that it was all sweetness and light. Trust was sometimes gained because of the sanctions administered if one or another party did not deliver as

promised. Sometimes the sanctions could be very tough and personal or sometimes the sanction was exclusion: The outcome was the same. In one way or the other, transactions and trade were carried out in an environment of trust and confidence.

History tells us that there cannot be trade and exchange, in effect an operational economy, without a working physical, legal and institutional infrastructure. It can be codified or involve a tacit understanding. But a shared understanding of the rules and sanctions has to exist.

And at the heart of each exchange is the trust that the product or service will be delivered as promised. Or that the medium of exchange - money - itself can be trusted.

It was understood, early on, that the soundness of the money was paramount. Consider that in England in 1108 under King Henry I, trust and confidence in money was achieved using very strong measures, "....false and bad money should be amended, so that he who was caught passing bad denarii should not escape by redeeming himself but should lose his eyes and members."**2**

Systems of credit were developed in the middle ages. Credit instruments morphed into paper money and chequing instruments developed as well. In the early 1500s, in Holland, the first cheques came into widespread use. A system of weights and measures, one that could be trusted, was developed and dates from the late 12th century.

The early history of commerce shows the many and varied ways in which standards, currencies and ways of behaving developed slowly over time to meet the needs of the day. The infrastructure of custom, rules, laws and regulations underlying and sustaining commerce grew slowly and organically.

A brief historical review reveals an important lesson from history, what can be called a verity: That some sort of regulation or oversight is needed in trading and transaction networks of all types. There must be some sort of functional arrangement that can administer sanctions for those who do not "play by the rules of the game". Whether the sanctions were harsh (imprisonment) or soft (exclusion), there was a realization and acceptance that if the activities were to be trusted then sanctions were necessary.

Sanctions and rules could either be explicit or implicit and were administered within a trading group (a closed group or network) or could be administered by an outside party, usually a regulatory or judicial agency of government (an open group or network).

LEARNING FROM THE PAST, COPING WITH THE FUTURE

Closed user groups are seen in an association of banks or airlines, or a crime cartel, whose members are linked by an existing business relationship. Such networks are usually self enforcing, governments have a minimal or no role in their operation and the public is usually rarely aware of either the working of the network or when sanctions are

2 http://www.fordham.edu/halsall/sbook.html

administered because of transgressions. An offline example is the network of diamond merchants of Amsterdam and London. An online example is the financial services network SWIFT (Society for Worldwide Interbank Financial Telecommunication) [22], which has for its members some 8,300 financial institutions in some 200 countries and largely works in the background facilitating the transactions of the members of the network (see Annex 1).

Open trading groups or networks require the intervention of some sort of outside agency, usually a regulatory agency or policing function of government. This is required to create and enforce standards and to regulate the behaviour of those using the network.

Over time robust infrastructures grew organically and were slowly adapted for each of the major technologically driven transformations. The railway, telegraphy, the telephone, the banking system, the automobile, each had to "grow" its own infrastructure, adapting from earlier events and developing new institutions and legal and physical manifestations to meet the changing needs of the new environment.

Each infrastructure rested on, was enabled by and/or depended on a range of regulatory and administrative agencies which were created to provide oversight, equity, access and to ensure the smooth functioning of the infrastructure. There was always an oversight body of some type, either internal or external, that could administer either "soft" or "hard" sanctions to ensure that trust was maintained. Consider, for example, the alphabet soup of regulatory and oversight agencies in the U.S. such as ICC, FAA, CAB, FCC, SEC, NHSTA and many more, that were put in place to ensure the health of the infrastructure.

It is in this context that the infrastructure for the networked economy/society must be considered. Closed user group networks such as SWIFT can handle things very much on their own. (see Annex 1). Issues arise when we turn to open networks such as the Internet. The public Internet, a global network of over 50,000 loosely connected networks spanning every country, has no regulatory or oversight government agency that can administer sanctions when the "rules of the road" are violated. In fact, widely agreed upon "rules of the road" have yet to be developed! What new institutional arrangements (regulatory and oversight) might be necessary if we are to have in place an understandable, predictable and respected Internet-based infrastructure?

The industrial economy achieved a stable institutional framework and communications infrastructure, with "rules of the road" built on national postal, telegraph and telephone systems. These were linked together by international institutions such as the Universal Postal Union (UPU) and the International Telecommunications Union (ITU), currently the two oldest UN Agencies, to give them global reach. In a previous paper [15], the authors noted that a similar infrastructure, which we have called the cyber-infrastructure, must be created for the new digital economy. Such an infrastructure would be 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 digital economy and society.

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, because there were entities tasked with fulfilling these responsibilities and empowered to do so. These entities - the "Theys"- can intervene if rules, written or unwritten, are breached.

The Internet has evolved at an unprecedented rate and since it consists of an agglomeration of autonomous networks bound together by the Internet Protocol, it has characteristics quite unlike those of the earlier trusted networks. One characteristic of the public Internet is that it has no well defined "they". 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. While users may think that Internet Service Providers (ISPs) are tasked with this responsibility, it is not clear that they are empowered to do so or are even required by law in various jurisdictions.

The Internet, as an open network where there is no outside body that can administer sanctions, appears to be unique in commercial history.

ISSUES AND CHALLENGES: ESTABLISHING AN ENVIRONMENT OF TRUST AND CONFIDENCE

> "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.
>
> "Governments, businesses and civil society should work closely together to ensure that trust, security and privacy are as fully secured on the internet as they are in the real world".
> The Declaration of Amsterdam "The Digital Road to Recovery". World Congress on Information Technology 2010, Amsterdam, May 25-27, 2010. Available at

The very success of the Internet as an economic tool and its ubiquity has led 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 [13] 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. Concerns regarding security from hackers and phishers, identity theft, congestion caused by spam and differentiated qualities of service were not matters of major concern to the early designers and implementers of the Internet. These matters came to the fore after the Internet began to evolve into a ubiquitous commercial medium. It is a profound challenge to retrofit the Internet with the necessary safeguards and oversight mechanisms while it continues to expand rapidly.

Issues

> *"… the Internet needs to be secure. Just as we have to keep our shipping lanes free from pirates, we need to keep our digital thoroughfares open and free from cyber-threats".*
> Ivan G. Seidenberg, Chairman of the Board and Chief Executive Officer of Verizon, Speech to the Council on Foreign Relations, New York, April 6, 2010

We are slowly getting used to the fact that the public space of the Internet can be a "dark and dangerous" street with many unsavory actors wanting to cheat us with scams [5], threaten us with cyber-crimes like fraud, identity theft, etc [4], [5], harass us with spam [9] 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. Some are choosing not to go online, even to go to a secure private space such as online banking. 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.

There are, however, secure sites on the Internet. Instead of urls starting with the familiar HTTP, they are easily identified by the letters HTTPS. The "S" indicates that the website in question (usually one where transactions can take place) is secure. Security is achieved through a protocol called Secure Sockets Layer (SSL) which uses encryption and identification of all parties so that anonymity is eliminated. The main idea of HTTPS is to create a secure channel over an insecure network. To get this status the website has to get a certificate (good for one year) from a trusted third party provider that ensures that the website in question is valid.

SSL is used more and more and goes some way to providing trust and security for a variety of transactions. But while it may make certain online "stores" safe for transactions, the online "streets" are still open, anonymous and potentially unsafe. And some analysts have wondered how long it will be before SSL-protected websites are also phished: This means that a phoney HTTPS is created so that unsuspecting shoppers enter their identifiers, passwords and credit card information to a false clone of the real thing.

Online banking tries to 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 (phishing and pharming)?

Trust and confidence are crucial to effective economic functioning. What are some of the mechanisms at work when trust is present?

Trust promotes economic efficiency by reducing the transaction costs of economic exchange, on the assumption that others will behave according to common norms of economic conduct. Going further, when trust is absent or is lacking it is possible to measure or consider the costs of distrust. For example, consider the many lawyers and notarized documents needed when, with trust, only a handshake is needed.

Of course it is possible to have transactions when trust is lacking but the process is usually not smooth and it is often quite costly, either in lawyers fees before the fact or in lawsuits after the fact. Resort to law is costly – transaction costs are minimized when ordinary economic business is done under an implicit rather than an explicit contract.

Trust matters for economic life, in the tacit assumptions we make that others share our understanding of an exchange, are operating according to common social norms: trust mediates the risk inherent in an economic transaction. The reduction of economic uncertainty, the "oiling" of exchange relations, the management of risk, all help to foster economic efficiency. Thus trust leads a double life as both a social value and an economic resource. [17].

Living in a world of distrust is costly. Every transaction is burdened with the cost of authentication and verification, through the use of elaborate procedures which impose both costs and delays. This is as true for the online world, as it held true earlier 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. Policymakers should examine these past successful systems and networks, to see what lessons can be learned for the implementation of a robust cyber-infrastructure to serve the needs of a digital economy.

We contend that a successful cyber-infrastructure cannot be achieved on a shaky foundation of trust. Unless steps are taken to increase trust and confidence, then full participation by citizens in an online world is unlikely. A variety of technical solutions such as linking individuals to unique IP addresses is compelling. However, unless there is an oversight mechanism, a "they", to administer sanctions as necessary, such a fix will not solve the problems.

A "They" and a "Who"

We have identified the need for a "They" but have not addressed the corollary; the need to identify a "who". An effective oversight mechanism can only function if it can identify those who transgress. Who is it that is involved in spam, identity theft, hacking, or other aspects of cyber-crime?

Anonymity has been a valued aspect of the Internet world, even though those who frequent social groups often give up such anonymity (whether they know it or not and

whether they care or not.)

But for trust and confidence to take hold there must be some way of identifying users who are parties to a transaction. Think, for example, if cars had no license plates. A speeder or someone involved in an accident could not be caught or charged. The existence of a “They” is fine in the abstract but without the ability to identify a “Who” (the miscreant) the threat of sanctions rings rather hollow.

A novel suggestion to address this issue was made by Craig Mundie, the chief research and technology officer at Microsoft. During a presentation at the 2010 World Economic Forum in Davos, he suggested that consideration be given to driver’s licenses for the Internet. Mundie’s concerns echo those of the authors of this paper. As he noted, anyone can get online and no one has to say who they are. We can figure out where the particular attacking machine is located, but there is really no way to go back one step further and track the identity of the computer that hacked into the one that hacked into you!

What Mundie is proposing is a way to achieve authentication. He draws an analogy to the automobile. A license for the vehicle, and a driver’s license. Mundie imagines three tiers of Internet ID: one for people, one for machines and one for programs (which often act as proxies for the other two).

For those who say: We're entitled to anonymity on the Internet the answer can only be, Really? Why do you think that?

Mundie points out that in the physical world we are comfortable with the notion that there are certain places we’re not allowed to go without identifying ourselves. On the street no ID is necessary. Walk into a bank vault and you must give your name and establish that you have authorized access. He suggests that it is just a matter of time before some sort of identifier will be needed for people, machines and programmes if one wants to travel the information highway.

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. 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 agreement and acceptance of both broad and specific governance approaches aimed at buttressing the vital areas of trust and confidence.

Parts of the cyber-infrastructure are in place now, but more is needed. All stakeholders must become more aware and knowledgeable about the need for a secure and trusted 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 cyber-infrastructure 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.

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.

Socio-economic Impacts of Malware and Cyber-crime

The total economic cost associated with high-tech crime in Canada, or affecting Canadians abroad, is largely unknown. Canada currently does not have a uniform method of collecting statistical data on this new category of criminal activity in either the private or public sector but figures from a variety of sources indicate that the magnitude of the problem is astounding [3], [5], [11].

A recent study carried out by Information Week Research for PricewaterhouseCoopers, covering 30 countries and some 5,000 IT professionals, estimates that hacking, Internet fraud, denial of service attacks and high-tech mischief cost the world economy some US$1.6 trillion dollars a year in loss of business revenue and damage to computer equipment and data. [11]. **http://www.ecommercetimes.com/story/3741.html**

The Canadian Anti-Fraud Centre reported 7778 cases of identity theft in 2006, resulting in millions of dollars in damages. [5] **http://gcsc.org/index.php/public/cybercrime/**

The Canadian Council of Better Business Bureaus has estimated that identity theft may cost Canadian consumers, banks, credit card firms, stores and other businesses more than $2 billion annually. [3], [5] **http://mbc.app.bbb.org/tips?id=104**

2007 research from the U.S. Cyber Consequences Unit shows that the destruction from a single wave of cyber attacks on critical infrastructures could exceed US$700 billion – the equivalent of 50 major hurricanes hitting the U.S. soil at once. [5] **http://www.therawfeed.com/2007/08/one-cyber-attack-could-cost-700-billion.html**

Earlier this year ***The Washington Post*** [**24**] reported on a massive computer attack, involving more than 75,000 computer systems at nearly 2,500 companies in the United States and around the world. The attack targeted proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology industries. The hackers lured unsuspecting employees to download infected software, or baited them into opening e-mails containing the infected attachments. If the employee fell for the ruse, malicious software embedded in the sites or the e-mails enabled the attackers to commandeer users' computers, scrape them for log-in credentials and passwords - including online banking and social networking sites - and then exploit that data to hack into the systems of other users. The attack's scale demonstrates the increasing sophistication of the cyber-criminals involved and has highlighted the inability of the private sector, including industries that would be expected to employ the most sophisticated cyber defenses, to protect itself.

Debit card fraud is practically an epidemic, although the Canadian Bankers Association and the Interac Association bristle at the suggestion. According to Interac, in 2009 the reported amount lost to debit-card fraud was $143.3 million, a 40% jump from $104.5 million in 2008. [12]

In late January 2010 ***FOX News*** reported that social network users can expect a veritable tidal wave of spam as cyber criminals are increasingly targeting social networking sites like Facebook and MySpace. Cisco Systems has estimated that, as a result, worldwide spam volumes could rise by 30 to 40%. One of the more popular scams utilized by spammers are phishing attacks that lure unsuspecting victims to click on links that download malicious software onto their computers to steal personal information including banking details and passwords. Interestingly, just two years ago there were virtually no Facebook phishing messages. However, today Facebook ranks as the second most phished organization online and, if current trends continue, is on track to take the top spot in 2010.

The growth of electronic commerce and the use of the Internet by particularly vulnerable demographic groups such as children and seniors is believed to have accelerated the growth rates of tech crimes in the last few years. There is little reason to expect this rampant growth to slow without a concerted policing, legislative and research effort to rein in high tech criminals and their secretive networks.

Challenge: The Need to Create Trust and Confidence in an Online World

> "Trust is so much a part of the fabric of our society that we only notice it when it has been abridged or lost"
> (Anon)

Trust is something like electricity: We only notice how important it is when there is a power failure. Then we realize that the lights have gone out and the elevators aren't working and the HVAC systems are down and high rise buildings are uninhabitable and our computers are down and so on. It is the same with trust. We assume that trust is present and only truly understand its loss when it has been abridged in one way or another.

There is a cost to distrust and this is the efficient functioning of the economy itself. When trust is lost transactions become almost impossible.

Trust can take a long time to create, but can be eliminated in an instant. The old saying, "Fool me once, shame on you, fool me twice, shame on me" means that after having had one's trust violated a second time, the individual is likely to withdraw from transactions concerning an individual, an institution or perhaps using a particular medium of communication for the transaction–the Internet.

As noted in the quote by Henry Ward Beecher at the preface to this paper,. ". commerce dies the moment, and is sick in the degree in which men cannot trust each other".

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.

The task of building an environment of trust in the digital economy is complex. 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 [15], [16]. 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. The additional constraint is that a retrofit is needed as soon as possible, and that all players should "more or less" agree on the nature of the retrofit.

MEETING THE CHALLENGES

> "…We enter this new decade recognizing that we rely on the Internet for essential social purposes: health, energy efficiency, and education. It's also a general engine for economic and social innovation. We must take rules more seriously if we want full participation, but we must keep the need for flexibility in mind…" Remarks of Lawrence E. Strickling, Administrator of the U.S. National Telecommunications and Information Administration, to The Media Institute, February 24, 2010.

There have been discussions on the Internet about what sort of regulation is needed or desirable. Ideas range from cyber-anarchy, to self-regulation , to designing ways of behaving into the network in the form of code (e.g., the notion that code is law, cf. Lessig [14]), to more traditional regulatory mechanisms associated with past, successful communications systems (viz. postal services, telegraphy, telephony). This new technology will have its own unique regulatory framework. But it will only flourish if there is some agreement and acceptance of both broad and specific governance approaches, and that there is agreement on a "They" which would imply the existence of mechanisms of governance, oversight and sanctions. Also, of course, that there is agreement on how to identify those who transgress, so that sanctions can be imposed when required. What is needed are ways to identify the "who".

The Role of Governments

> "…I say that the government's role need not be one of a heavy-handed regulator... But it concerns me that in the absence of some level of government involvement, we will lose the one thing that the Internet must have—not just to thrive, but to survive—the trust of all actors on the Internet…"
> Remarks of Lawrence E. Strickling, Administrator of the U.S. National Telecommunications and Information Administration, to The Media Institute, February 24, 2010.

The historical role of governments in ensuring the orderly implementation of broad, general purpose technologies (GPTs) 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.

Governments 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.

One National Response: The example of Canada

> "Canadian shoppers should feel just as confident in the electronic marketplace as they do at the corner store…with today's two pieces of legislation, we are working towards a safer and more secure online environment for both consumers and businesses."
> Remarks by The Hon. Tony Clement, Minister of Industry, when introducing Bill-C-28 and Bill-C-29 to the Parliament of Canada on May 25, 2010 [7,8].

> "Policy and legislative tools to protect personal information and ensure secure transactions are key to building and maintaining trust and confidence in the online marketplace".
> Digital Economy Strategy Consultation Paper, May 10, 2010 [6]

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. We offer the following as an illustrative of the approach taken in one country, Canada.

Canada has developed a "shopping list" of what sorts of things are needed if trust and confidence is to prevail in the electronic marketplace. One of the key objectives of Canada's Electronic Commerce Strategy [10] 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. 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;
- 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;
- protect individuals and businesses against annoying or abusive practices, such as unsolicited bulk e-mail (spam);
- ensure that networks are secure and operate reliably.

This is still a work in progress. Some of these measures are in place, while work is continuing on others.

At the federal level, the legislative framework for trust and confidence began with the development of the Personal Information Protection and Electronic Documents Act (PIPEDA) [8]. The Act, which came into effect in 2001, is Canada's federal private sector privacy law. It was established largely in response to consumer concerns about the need to protect personal information in the context of electronic commerce. PIPEDA was enacted to support and promote electronic commerce by protecting personal information that is collected, used or disclosed during the course of commercial activities.

There is a statutory requirement for PIPEDA to be reviewed every five years. Following its first statutory review, PIPEDA will be amended through Bill C-29 [8], introduced on May 25, 2010, to enhance privacy in the digital age by better protecting and empowering consumers, clarifying and streamlining rules for business, and enabling effective law enforcement. Several of the proposed amendments will make a significant contribution to the government's efforts to maintain a safe and secure Internet experience for Canadians, including new data breach notification requirements and enhanced consent provisions to help ensure privacy protection of children online. Once completed, the amendments will ensure Canadian privacy legislation continues to be a world-class model of privacy law.

In addition to the amendment of PIPEDA, the Government of Canada is putting in place a modern and efficient legal framework to protect the online marketplace and better protect Canadians from cyber-crime. It has started with the reintroduction on May 25, 2010 of Bill C28, the proposed "Fighting Internet and Wireless Spam Act (FISA)" [7], aimed at deterring the most damaging and deceptive forms of spam and related online threats from occurring in Canada, and with the creation of three new Criminal Code offences under An Act to Amend the Criminal Code. These came into force on January 8, 2010, providing police and justice officials with important new tools in the fight against identity theft. In addition, two complementary legislative initiatives aimed at enhancing law enforcement's ability to combat cyber-facilitated crime and modernizing investigative techniques, along with actions to better protect children from Internet luring and cyber abuse, remain priorities of the federal government.

The development of tough anti-spam legislation (FISA), together with proposed amendments to PIPEDA and other legislative measures described above, are aimed at providing assurances about the security, integrity and reliability of transactions, and are key to the continued growth of the online economy. These complementary pieces of legislation will be the foundation of a world-class Canadian legal framework for the digital economy. However, in an open, inter-connected and inter-dependent world, an "electronic moat" cannot be built around national borders.

International Collaboration

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, domestic rule-making will have limited effectiveness. Thus, in order to meet national policy objectives 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.

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 could 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.

Spam and identity theft have been the subject of legislative and regulatory action in the U.S. [23], 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 such as these require concerted action by governments and the private sector aimed at establishing practical rules of the game, and cooperative enforcement. Protecting customer information and preventing identity theft are key to meeting growing security problems. Governments must take the necessary legislative steps to effectively address these issues.
An analogy can be drawn to the start of the 20th century, when the business infrastructure was based on letters carried by the national postal system, and telegrams transmitted by postal systems or regulated entities like Western Union in the US. *If every three or four letters and telegrams out of five had been fraudulent, could these business practices have continued?* Signed letters and telegrams had standing in the courts of law; tampering with the mail in the US was (and still is) a criminal offence.

An earlier Pew Foundation study [20] 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 (see Annex 1), 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. An analogy would be registered mail, for

those who require it and are willing to pay, moving on to first, second and third class mail - less cost, less security.

So serious is the threat of spam and cyber-crime that cooperative, multi-jurisdictional enforcement of civil and criminal sanctions will be required to stem the tide. Due to the borderless nature of electronic markets and services, such marketplace rules must work both domestically and across international boundaries. 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

Findings

Although the Internet has transformed the economy, society and politics, it was never designed and built for global, ubiquitous and secure commercial use. While the technology is new, the need for trust, confidence and security remains.

As noted above, there are secure sites on the Internet. HTTPS designates these SSL-protected sites used for online banking and a variety of transactions. But while great effort and expense has gone to make these sites secure, the Internet itself remains an open and largely ungoverned space.

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

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 a large agglomeration of autonomous and apparently self-regulating networks. However, currently 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. *This must be remedied*. As we have seen above, strict anonymity on the Internet compromises the ability of a “They” to impose sanctions on a “who” when required, since there is no facility to identify the “who”.

It will be 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. Though difficult to accomplish, this paper should be seen as an international “call to action” to start tackling this problem.

CONCLUSIONS

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 strong agreement and acceptance of both broad and specific governance approaches aimed at buttressing the vital areas of trust and confidence.

We conclude that a successful cyber-infrastructure cannot be achieved on a shaky foundation of trust. One cost of distrust would be the continuing erosion of confidence in the online world, with the eventual failure to harness the full potential of the Internet, for our economic, social and political well-being.

However governance of the Internet evolves, the authors hope that this paper has made the case that the status quo is untenable, if we hope to obtain the full benefits of a digital economy.

Glossary

Botnet (From robot network) is a term for one or more networks that have been created by inserting pieces of software into compromised computers. Compromised computers can be anywhere on the Internet. These computers, that can number in the thousands or hundreds of thousands, can be activated by a hacker (bot master) on command. When the command is given they will act as a dedicated network to perform a particular function. A common use of botnets is in denial of service attacks (see below).
http://en.wikipedia.org/wiki/Botnet

Cloud Computing Refers to applications, services and computing platforms offered over the Internet. These services are offered from servers located in data centers all over the world, which collectively are referred to as the "cloud." Software and information are provided to computers and other devices on-demand, like a public utility. This metaphor represents the intangible, yet universal nature of the Internet. The idea of the “cloud" simplifies the many network connections and computer systems involved in online services. In fact, many network diagrams use the image of a cloud to represent the Internet. This symbolizes the Internet's broad reach, while simplifying its complexity. Any user with an Internet connection can access the cloud and the services it provides. Details are abstracted from the users who no longer have a need to know about the technology infrastructure. It represents a maturation of the technology. As with earlier technologies, maturation is about “plug and play”. Turn the key or hit the switch and the technology meets the needs of the user.

Some examples of cloud computing include online backup services, social networking services, and webmail. Anyone can access their webmail from anywhere in the world simply by knowing the web address of the webmail service, there's no need to know the name of the server or an IP (Internet protocol) address or anything else. Both Google and Amazon are offering software services to users who just need to specify their project without having to delve into a host of technical details.
http://www.techterms.com/definition/cloudcomputing
http://www.bestpricecomputers.co.uk/glossary/cloud-computing.htm

DNS (Domain Name System) The reason the Domain Name System is used is because Web sites are actually located by their IP (Internet protocol) addresses. For example, when you type in "http://www.adobe.com," the computer doesn't immediately know that it should look for Adobe's Web site. Instead, it sends a request to the nearest DNS server, which finds the correct IP address for "adobe.com." Your computer then attempts to connect to the server with that IP number. DNS is just another one of the many features of the Internet that make it simple to use and we take for granted. The DNS keeps Web surfers sane and Web access simple. Without DNS, we would have to remember the IP address of every site we wanted to visit, instead of just the domain name. We would have to remember the address "17.254.3.183" instead of just the url "apple.com". Most users have an easier time remembering simple names rather than complex numerical IP addresses.
www.yuiop.com/glossary1.htm
http://www.docstoc.com/docs/15438962/Terminology-Quiz-%E2%80%93

DoS (Denial of Service) attack A denial of service (DoS) attack is one in which a multitude of compromised systems (including Botnets) attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially overloads the system and forces it to shut down, thereby denying service to and from the system to legitimate users. A hacker begins the attack by communicating with systems that have been compromised. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of messages to the target causes a denial of service.

While the press tends to focus on the target of DoS attacks as the victim, in reality there are many victims in a DDoS attack - the final target and as well the systems controlled by the intruder. DoS attacks are becoming more and more common today, hampering businesses, government agencies, and educational and medical institutions from performing their tasks effectively, safely, and efficiently. http://www.firewall.cx/dosattacks.php

Hacker The term is now commonly used to refer to someone who can gain unauthorized access to other computers. A hacker can "hack" his or her way through the security levels of a computer system or network. This can be as simple as figuring out somebody else's password or as complex as writing a custom program to break another computer's security software. Hackers are the reason software manufacturers release periodic "security updates" to their programs. Some large businesses and organizations receive multiple hacking attempts a day.
http://en.wikipedia.org/wiki/Hacker

Identity theft is a term used that is to refer to fraud that involves pretending to be someone else in order to steal money or get other benefits. The term is actually a misnomer, since it is clearly not possible to steal an identity - a more correct term is *identity fraud* or impersonation.

The person whose identity is used can suffer various consequences when he or she is held responsible for the perpetrator's actions. In many countries specific laws make it a crime to use another person's identity for personal gain.

Identity theft can occur in two ways. The thief uses personal information to open new accounts in the victim's name. The thief might open a new credit card account, establish cellular phone service, or open a new checking account in order to obtain blank checks. Or the thief can take over an existing account. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem. The Internet has made it easier for an identity thief to use the information they've stolen because transactions can be made without any personal interaction.
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci801871,00.html

Malware - Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the Web pages a user visits to personal information, such as credit card numbers.
http://www.techterms.com/definition/malware

Phishing is part of an identity theft scam in which "spammers" use an authentic-looking e-mail to trick recipients into providing personal information such as credit card numbers or social security numbers. It is the process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting or naïve public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication (such as SSL), it may require tremendous skill to detect that the website is fake.
http://en.wikipedia.org/wiki/Phishing

Pharming is yet another way hackers and cyber-criminals attempt to manipulate users on the Internet. While phishing attempts to capture personal information by getting users to visit a fake website, pharming redirects users to false websites without their even knowing it. While a typical website uses a domain name for its address, its actual location is determined by an IP address. When a user types a domain name into his or her Web browser's address field and hits enter, the domain name is translated into an IP address via a domain name server or DNS (see above). The Web browser then connects to the server at this IP address and loads the Web page data. After a user visits a certain website, the DNS entry for that site is often stored on the user's computer. This way, the computer does not have to keep accessing a DNS server whenever the user visits the website.

One way that pharming takes place is via an e-mail virus that "poisons" a user's local DNS information. It does this by modifying the DNS entries, or host files. For example, instead of having the IP address 17.254.3.183 direct to www.apple.com, it may direct to another website determined by the hacker. Pharmers can also poison entire DNS servers, which means any user that uses the affected DNS server will be redirected to the wrong website. Fortunately,

most DNS servers have security features to protect them against such attacks. Still, they are not necessarily immune, since hackers continue to find ways to gain access to them. While pharming is not as common as phishing, it can affect many more people at once. This is especially true if a large DNS server is modified.
http://www.yourdictionary.com/computer/pharming

Social Networking In the early 2000s, the Web became much more personal as social networking websites were introduced and embraced by the masses. Social networking websites allow users to be part of a virtual community. The two most popular sites are currently Facebook and MySpace. These websites provide users with simple tools to create a custom profile with text and pictures. A typical profile includes basic information about the user, at least one photograph, and possibly a blog (Web log) or other comments published by the user. After creating a profile, users can add friends, send messages to other users, and leave comments directly on friends' profiles. These features provide the building blocks for creating online communities. With social networking users can share their lives with other people. These websites also provide an important linking element between users that allows friends to communicate directly with each other.

However social networks have also attracted hackers who direct unsuspecting users to fake sites where identity theft and other fraud can take place. Phishers can grab a social networker's credentials via an email-borne or other attack, and then use their profile to email their friends within the social network. Those emails within the social network direct the friends (victims) to an exterior site that duplicates the social network. The victim may think he/she is on the social network, but they are not. Social networks spend much time and resources tracking down these phishing attacks. One virus protection company in a recent report said that social-networking sites are a treasure trove of personal data, listing information such as birthdays, location and employment history. Users of social networking websites are putting up a large amount of confidential information. And such personal information attracts cyber-criminals.

http://www.silicon.com/technology/security/2008/04/09/phishers-attack-social-networking-generation-39185353/

http://www.techterms.com/definition/socialnetworking

http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=218101868

Annex 1 - Closed and Open Networks: Governance and related issues

In this paper the authors have discussed the Internet as it is today and suggested ways in which it must be strengthened to make it a more robust vehicle if it is to fully a play a role as the infrastructure for a digital economy and society. The authors are considering the Internet of today and how it might look in the future.

The universe of networks can range at one end from the completely open, without management (no “they” and anonymous “whos”) to a completely closed (a clearly defined “they” and clearly identified “whos”). These two extremes are put forward as boundaries: All networks fall somewhere in between. The polar cases are rarely seen in everyday life, but it is useful to identify the possible range.

Different networks have been put in place to meet different needs. The very closed and closely managed networks - those put in place by the banks and military for example - meet one need. .Those networks with open access and lightly managed meet another need. Here the goal is to encourage entrance and participation. **Networks are matched to needs and there are tradeoffs in moving from one type of network to another**. Get something and give up something else.

In the bricks and mortar world we see these tradeoffs in our everyday lives but rarely stop to consider them.

Consider another area: Parking lots. Some parking lots are completely open. Cost nothing to park; there is no attendant; and the car is parked by the owner knowing that while the cost is free, the oversight is nil and damage or theft is possible: A trade-off. Or there can be an attendant who issues a ticket and payment is made and while the ticket has a disclaimer (“not responsible, etc., for damage, etc.”), there is an implicit assumption that there is oversight. Here anybody who pays to park can do so. Payment is the price of admission. Little or nothing is known about the driver except that he/she is willing to pay to park.

Ramping up to more security and more management, the parking lot can only be entered with a magnetic pass card. Here much can be encoded on the card and the lot is only open to those who pay and those content to give up information to get access. The user pays for security and the more closely managed lot is not open to the casual passerby. It is a closely managed lot with a well defined “they” and a well defined “who”.

Although the Internet has changed all our lives, it was simply never designed and 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 complementary but separate IP-based networks: One which is secure and managed, with security features built in from the beginning. The other more open, resembling the current public Internet. The authors suggest that the current configuration of the Internet is not secure enough to take on the role of infrastructure for the digital economy: It lacks the necessary attributes of trust and confidence.

It should be noted that the current "bricks and mortar" world provides 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. These options have evolved over time in an organic way and we rarely pause to consider what happens when we purchase something from a street vendor vs. what happens when we go inside a department store to purchase something. Different levels of security are present and a different "package" is purchased. The product doesn't work in one case and the street vendor is gone; the product doesn't work in the other case and the store exchanges the product or refunds the cash to the buyer.

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. If the Internet evolves in this way then rules of the road should be made explicit. Social networks carry one level of trust and security and commercial networks carry a different level of trust and security. Anonymity may be more acceptable on one network; less acceptable on the other. Users should know in advance the risks they are taking in going into one sort of network vs. another.

It is unfortunate to find out later that the transaction they thought was secure was not secure at all. That the web site they visited was phony and that some sort of virus was introduced merely be visiting what they thought was the familiar site of their bank or other familiar web site. And further there may be much consternation when it is learned that the authorities are of little help because while there is much spamming and hacking on the net, miscreants can't be tracked down because, well because we don't know who they are. They are anonymous and by using a variety of sophisticated devices have covered their computer tracks.

Some Current Examples of Closed and Open Networks

Closed Managed 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 Athey@ responsible for the design and operation, as well as policing the appropriate use of the network, and all members are well defined "whos".** Security is desired by all users. Many such private or closed user group networks are now converting, or have already converted to the IP standards to make them Internet accessible while maintaining or even enhancing the necessary operational functionality, reliability and security. 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.

Applications and Examples of Closed Managed Networks

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 8,830 institutions in 209 countries and territories [22]. SWIFT=s worldwide community includes banks, brokers/dealers and investment managers.

SWIFT has been in operation for over 35 years and the network has evolved continuously, to take advantage of technological advances

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.

Perhaps the most widely used online payment system is PayPal, (https://www.paypal.com), a Web based service that enables Internet users to send and receive payments electronically. PayPal, currently a wholly owned subsidiary of eBay, is an example of a payment intermediary service that facilitates worldwide e-commerce.To open a Pay Pal account, users register and provide their credit card details. When they decide to make a transaction via Pay Pal, their card is charged for the transfer. A PayPal account can be funded with an electronic debit from a bank account or by a credit card. The recipient of a PayPal transfer can either request a check from PayPal, establish their own PayPal deposit account or request a transfer to their bank account

Private sector joint ventures like SWIFT, Visa and MasterCard have helped to create a global electronic payments network, which is increasingly inter-linked to online transactional systems and serves as their payment vehicle. 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. By carefully constructing a network with well defined “theys” and “whos” a degree of trust and confidence was achieved. This has led to a safe, sound and predictable international payments network connecting buyers, sellers and financial institutions with ever-increasing levels of security. A case of carefully designing a network to meet a specific need.

Open Public Networks

Open networks, also referred to as open public networks**,** have no restrictions on membership and are open to use by anyone willing to pay the established tariffs and abide by certain policies for acceptable use. There can be campus networks or metropolitan area networks. Or other defined user group networks or geographically defined networks. Usually these networks offer access to the Internet. Oversight is usually minimal and where there is a problem or transgression of the rules there is usually 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 at some level of government. This is to create and enforce standards and to regulate the behaviour of those using the network. The public Internet, a global Anetwork-of-networks@ consisting of over 50,000 autonomous, loosely connected, IP-based networks spanning every country, is currently the best known example of an open network.

The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own standards. Only the Internet Protocol address space and the Domain Name System, are controlled by an organization, the

Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely-affiliated international participants that anyone may associate with by contributing technical expertise.

Thus 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 Athey@, 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 statutory authority and power to Apolice@ the public Internet.

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" that can administer sanctions when transgressions occur. As we have noted in the body of the paper, a “They” is a necessary but not sufficient condition for effective governance. Needed also is an identifiable “Who”.

Going back to our analogy above, the Internet is more akin to an open public parking lot. Standardized spaces for cars are marked off. Entrance and exit from the lot is clearly demarcated. The asphalt and underpinnings for the lot are secure. What the various parkers do is not regulated at all. If damage or theft occurs there is little that can be done since the “publicness” of the area means that “theys” and “whos” are absent or are only present in the vaguest sort of way.

Next Generation Networks and Cloud Computing

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 by the authors in earlier papers [15[,[16], 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 or even multi-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.

Perhaps this is a logical development since in the current “bricks and mortar world” there are a variety of closed and open spaces that are accessible to the individual. The sidewalk is open, but step into an office building and a variety of security interfaces are met if one is go beyond the lobby to the offices within the building. The security is different in different buildings: e.g., entering a building with offices which have public interaction (lawyers, accountants, etc.) vs. buildings housing banks or stock trading.

As we have seen, using encrypted networks (SSL and HTTPS) there are islands of security in the largely insecure, open Internet network.

The telecommunications carriers claim that their new all-IP Next Generation Networks (NGNs) would be able to meet these needs. Similar claims are beginning to be made by the proponents of Cloud Computing, which is being billed by firms like IBM, Google and Amazon at the next computing paradigm.

Whether a multi-tier Internet is a desirable solution, from a public policy and welfare point of view, needs to be debated further. Its opponents claim that this Awalled garden@ approach would lead to the balkanization of the Internet. Its proponents claim that without network tiering, users with critical requirements like security or guaranteed Quality of Service (QoS), will gradually abandon the public Internet for Closed User Group networks which can satisfy such requirements, on a customized basis. However the Internet evolves, towards a multi-tiered network or some other model, the authors hope that this paper has made the case that the status quo is untenable, if we hope to obtain the full benefits of a digital economy.

References

(1) APWG (Anti-Phishing Working Group) (2009*) "Phishing Activity Trends Report",* 4Q 2009, 3Q 2009.
Available at http://www.antiphishing.org

(2) Atkinson, R.D. and McKay, A.S. (2007) *"Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution",* The Information Technology and Innovation Foundation (ITIF), Washington, D.C., March 2007. Available at http://www.itif.org/files/digital_prosperity.pdf

(3) Canadian Council of Better Business Bureaus (2010) "Consumer Tips – Identity Theft". Available at http://mbc.app.bbb.org/tips?id=104

(4) 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/

(5) Global Centre for Securing Cyberspace (GCSC) (2010) "About Cybercrime". Available at http://gcsc.org/index.php/public/cybercrime/

(6) Industry Canada (2010) "*Improving Canada's Digital Advantage: Strategies for Sustainable Prosperity*", Consultation Paper for a Digital Economy Strategy for Canada, launched on May 10, 2010. Available at http://www.digitaleconomy.gc.ca .

(7) Industry Canada (2010): *Bill C28,* the proposed *"Fighting Internet and Wireless Spam Act (FISA)"*. Bill introduced to the Parliament of Canada on May 25, 2010.

(8) Industry Canada (2010): *Bill C-29*, the proposed amendments to the "*Personal Information Protection and Electronic Documents Act* (PIPEDA)". Amendments to the Statute proposed as a result of its first mandatory review. Bill introduced to the Parliament of Canada on May 25, 2010.

(9) Industry Canada (2005) *Stopping Spam: Creating a Stronger, Safer Internet*, Report of the Ministerial Task Force on Spam, May 2005. Available at http://www.e-com.ic.gc.ca .

(10) Industry Canada (1998*) The Canadian Electronic Commerce Strategy*, Ottawa, September 1998. Available at http://www.e-com.ic.gc.ca

(11) Information Week Research Report (2010) "*Year's Hack Attacks to Cost $1.6 Trillion*". Study of 30 countries and 5,000 IT professionals, carried out for PriceWaterhouseCoopers. Available at http://www.ecommercetimes.com/story/3741.html

(12) Interac Association - A recognized leader in debit card services, Interac Association is responsible for the development and operations of the Inter-Member Network (IMN), a national payment network that allows Canadians to access their money through Automated Banking Machines and Point-of-Sale terminals across Canada. See http://www.interac.ca/about.php

(13) Internet Society *A Brief History of the Internet,* available at http://www.isoc.org/internet/history/brief.shtml

(14) Lessig, Lawerence (2000) *Code and Other Laws of Cyberspace,* Basic Books, 2000.

(15) Neogi, P.K., Cordell, A.J. (2005) *"Trust and Confidence and the Digital Economy: Issues and Challenges",* Journal of Internet Banking and Commerce, Vol. 10, No. 2, Summer 2005.

(16) 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.

(17) Intereconomics (2009): "*Trust, Confidence and Economic Crisis",* Intereconomics, July/August 2009. Available at www.ceps.be/system/files/book/.../44-4/196-202-Tonkiss.pdf

(18) OECD (2009) "*Cloud Computing and Public Policy*", Briefing Paper for the ICCP 2009 Technology Foresight Forum "Cloud Computing: The Next Computing Paradigm", Paris, October 14, 2009.
Available at
http://www.oecd.org/document/38/0,3343,en_2649_34223_43921574_1_1_1_1,00.html

(19) OECD (2008) *The Seoul Declaration for the Future of the Internet Economy* OECD Ministerial Meeting on the Future of the Internet Economy, June 2008. Available at http://www.oecd.org/futureinternet/.

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

(21) Statistics Canada (2007) *Canadian Internet Use Survey@*, 2007. The Daily, Catalogue No. 11-001-XIE. Available at http://www.statcan.ca

(22) SWIFT (Society for Worldwide Interbank Financial Telecommunication) (2008) *SWIFT Annual Report 2008 Shared Strength*. Available at
http://www.swift.com/about_swift/publications/annual_reports/SWIFT_Annual_report_2008.pdf

(23) U.S. CANSPAM Act (2003) *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003).* Available at
http://www.legalarchiver.org/cs.htm
Also see http://en.wikipedia.org/wiki/CAN-SPAM_Act_of_2003

(24) Washington Post (2010) "More than 75,000 computer systems hacked in one of the largest cyber attacks, security firm says", February 18, 2010.

(25) World Summit on the Information Society-Working Group on Internet Governance (WSIS WGIG) (2005) *Report of the Working Group on Internet Governance*, released July 14, 2005.

See also the Internet Governance Forum (IGF), set up by the UN Secretary General to provide a forum for multi-stakeholder policy dialogue on issues related to the Internet. Available at the official IGF web site http://www.wgig.org/