



World Information Technology and Services Alliance Public Policy Report 2001

**David A. Olive
Public Policy Chairman**

WITSA Public Policy Report 2001

- I. [INTRODUCTION](#)
- II. [FACILITATING THE DIGITAL ECONOMY](#)
- III. [IDENTIFYING E-COMMERCE BARRIERS](#)
- IV. [PRIVACY](#)
- V. [INFORMATION SECURITY](#)
- VI. [IT WORKFORCE ISSUES](#)
- VII. [TAXATION And TARIFFs in an E-COMMERCE ENVIRONMENT](#)
- VIII. [E-GOVERNMENT](#)
- IX. [INTERNATIONAL TRADE NEGOTIATIONS](#)
- X. [SEIZING DIGITAL OPPORTUNITIES](#)
- XI. [INTERNET GOVERNANCE](#)

FOREWORD

The World Information Technology and Services Alliance (WITSA) is a consortium of information technology (IT) industry associations from economies around the world. As the global voice of the IT industry, WITSA is dedicated to:

- advocating policies that advance the industry's growth and development;
- facilitating international trade and investment in IT products and services;
- strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information;
- providing members with a vast network of contacts in nearly every geographic region of the world;
- hosting the World Congress on IT, the only industry sponsored global IT event;
- hosting the Global Public Policy Conference; and
- hosting the Global Information Security Summit.

Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active *advocacy role in international public policy* issues affecting the creation of a robust global information infrastructure, including:

- **increasing competition** through open markets and regulatory reform;
- protecting **intellectual property**;
- encouraging cross-industry and government cooperation to enhance **information security**;
- bridging the education and **skills gap**
- **reducing tariff and non-tariff trade barriers** to IT goods and services; and
- safeguarding the viability and continued growth of the **Internet** and **electronic commerce**.

WITSA has a real impact on the global IT environment. It strengthens the industry at large by promoting a level playing field and by voicing the concerns of the international IT community in multilateral organizations, including the World Trade Organization (WTO), the Organization for Economic Cooperation and Development, the G-8 and other international fora where policies affecting industry interests are developed. WITSA recently issued statements on the WTO Agreement on Basic Telecommunications Services, the Year 2000, and electronic commerce.

This policy book is a summary of the positions taken by WITSA on global IT issues. These papers have been used by the industry in our dialogue with governments and multilateral institutions concerning their decision-making process with regard to important issues of concern to the IT industry, including e-

commerce, information security and privacy, taxation, e-government, and workforce issues. Full versions of WITSA's statements can be found at <http://www.witsa.org/papers/>.

I. INTRODUCTION

With over 200 million users online to the Internet world-wide, electronic commerce now accounts for a growing proportion of world trade. The Internet business model, which gives suppliers direct access to customers and new levels of efficiency with less assets and lower management overheads, is being eagerly investigated by major corporations. The emergence of global networks has already begun to influence the way individuals interact with each other, businesses conduct their affairs, and governments provide services to their citizens. WITSA's bench-mark study, the Digital Planet, revealed that total spending on information and communication technology (ICT) in 1999 exceeded U.S. \$2.1 trillion, and is expected to exceed U.S. \$3 trillion by 2003. The total value of Internet purchases in 1999 rose to U.S. \$130 billion, a figure projected in the Digital Planet to reach \$2.5 trillion by 2004. As with traditional commerce, electronic commerce requires trust across the whole spectrum of users and providers of services and goods. The radical changes brought about by the emergence of open networks will, in some instances, require modifications to the existing framework of rules to assure this trust. In some cases, new rules will be needed.

Throughout history, business has set its own standard rules and practices through a variety of organizations to lower transaction costs, to avoid and resolve conflicts, and to create consumer confidence. Today's commercial transactions are governed by a mix of laws enacted by government and business self-regulatory mechanisms. Governments have long acknowledged the fact that a dynamic trading environment requires a cautious approach to regulation and thus have traditionally welcomed business self-regulatory initiatives as the foundation of the rules governing commerce

The pace of change and emerging state of electronic commerce has heightened the risks associated with premature or unnecessary government regulation. This has increased the responsibility of business to promote a trustworthy environment through self-regulation and technological innovation. Business has a strong market incentive to foster the empowerment of users, but can only make the necessary infrastructure investments if it can trust that governments will recognize and reinforce the leadership of business in responding to the highly dynamic nature of electronic commerce.

Whereas today's framework of rules for the old economy business model have been developed and refined over many decades in an organic fashion, the consensus for global rules for electronic commerce is to move quickly in reviewing how, where and when new rules are necessary. As these rules must take into account the constantly evolving and inherently international nature of electronic commerce, any changes should be implemented only after a thorough discussion with all the parties involved and governments should support business-led rules development where possible. Business is working through its organizations to modify existing rules to ensure an efficient transition from paper-based to electronic commerce.

Should government regulation be necessary, the regulations ought to be internationally coordinated, as incompatible national laws create a fragmented global market with significant uncertainty as to what rules apply. In addition, extraterritorial application of a country's laws - and claims for far reaching application of a country's regulatory schemes - poses a significant problem to business, users and consumers and is a threat to electronic commerce. Therefore, non-discriminatory treatment of regulatory schemes affecting electronic commerce (e.g., financial industry including capital and securities markets, financial services, insurance and banking, transport, advertising, consumer protection schemes, taxes) is crucial. Jurisdiction, choice of law agreements, and enforcement issues must be dealt with in a responsible manner and with full involvement of commercial actors.

II. FACILITATING THE DIGITAL ECONOMY

WITSA has developed the following list of fundamental principles to be observed if the promises of electronic commerce are to be fulfilled¹:

- ❑ **Industry leadership:** The development of electronic commerce should be led primarily by the private sector in response to market forces.
- ❑ **Consistent legal and regulatory environment:** Government intervention, when required, should promote a stable, international legal and regulatory environment, allow a rational allocation of scarce resources and protect general interest. Such intervention should be no more than is essential and should be clear, transparent, objective, non-discriminatory, proportional, flexible, and technologically neutral.
- ❑ **Private sector participation:** Mechanisms for private sector input and involvement in policymaking should be promoted and widely used in all countries and international fora.
- ❑ **Technical standards:** In recognition of the global nature of electronic commerce, government policies that affect it should be internationally coordinated and compatible, and those policies should facilitate interoperability within an international, voluntary and consensus-based environment for standards setting. Governments should promote market driven standards and technical regulations. The standards environment should be voluntary and self-regulatory. Governments must negotiate mutual recognition agreements to remove duplicative testing and certification requirements and enshrine the principle ‘one standard, one test’.
- ❑ **Tax treatment:** Transactions conducted using electronic commerce should receive neutral tax treatment in comparison to transactions using non-electronic means. Taxation of electronic commerce should be consistent with established, internationally accepted practices, and administered in the least burdensome manner.
- ❑ **Telecommunications:** Regulation of the underlying telecommunications infrastructure, when necessary, should reduce impediments to competition, enabling new services and new entrants to compete, globally, in an open and fair market.
- ❑ **Competition:** Participation in electronic commerce should be pursued through an open and competitive market.
- ❑ **Security:** Government should not impose import or export controls on encryption products or attempt to force the use of government mandated management infrastructures. Users must have confidence that their communications are secure and private. Access to products with strong encryption capabilities is critical to providing this confidence
- ❑ **Effective intellectual property protection** and enforcement are essential for electronic commerce. Existing intellectual property laws need to be applied in the digital environment. Some aspects of copyright will require re-examination to insure that the degree of liability is related to the degree knowledge and control a party has in determining the content of a communication or web site. For example, Internet service providers who merely transmit or facilitate the transmission of information should not be held responsible for its content, of which they are unaware, and should not be required to monitor web sites and other digital communications.
- ❑ **The protection of users**, in particular concerning privacy, confidentiality, anonymity and content control should be pursued through policies driven by choice, individual empowerment, industry-led solutions, and should be in accordance with law where applicable. User empowerment including technology based filtering and rating systems are far more effective than sweeping regulations prohibiting or controlling access. Governments should rely on existing consumer protection legislation and processes as far as possible. New laws, specific to electronic commerce should be developed cautiously, keeping in mind the need to balance protection with not inhibiting growth.

¹ Initial work by WITSA on e-commerce is reflected in its statement entitled “Facilitating the Digital Economy” (May 1998). Concurrent work was conducted jointly between WITSA and the Alliance for Global Business (AGB): See “Discussion Paper On Trade-Related Aspects of Electronic Commerce” (April 1999) and “Global Action Plan for Electronic Commerce” (September 1998 & October 1999 editions).

- ❑ **Self-regulation:** Business should make available to users the means to exercise choice with respect to privacy, confidentiality, content control, and, under appropriate circumstances, anonymity.
- ❑ **A high level of trust** in the Global Information Infrastructure-Global Information Society (GII-GIS) should be pursued by mutual agreement, education, further technological innovations to enhance security and reliability, adoption of adequate dispute resolution mechanisms, and private sector self-regulation.
- ❑ **Cultural issues:** Governments should give priority to promoting cultural identity, rather than regulating content by quotas and other protectionist measures.

III. IDENTIFYING E-COMMERCE BARRIERS

The WITSA International [Survey](#) of Electronic Commerce 2000 reveals that the biggest hurdle facing the electronic commerce industry is a lack of trust of the new business channel. Of the 28 national WITSA member associations that took part in the enquiry into the issues facing the electronic commerce business, over a quarter identified ignorance about the medium as one of the most significant barriers to its development ahead of difficulties with technology, taxes, availability of skilled workers and regulatory issues. The results of this study show that the information technology industry and regulatory bodies have much work still to do before electronic commerce achieves its full potential. In particular, the survey identified eight issues that need special attention:

- ❑ **Trust** Security of payments is of paramount importance in the corporate acceptance, adoption and widespread deployment of electronic commerce. Developing countries cited low levels of credit card use and restrictions on using credit cards over the telephone as a problem in implementing consumer electronic commerce. Privacy ranked next among their concerns, followed by authentication – being sure of the identity and credentials of the party you are communicating with. Some three-quarters of the countries that took part in the survey believe that improving trust is vital to the development of electronic commerce.
- ❑ **Technology** Although Internet technology is still relatively new in many markets, WITSA members were confident that technical difficulties thrown up by a largely immature medium could be overcome. Respondents identified a wide range of technological barriers that need to be addressed. Top of the list was a need to make security systems more widely available and to ensure they are more widely used. Efforts to integrate electronic commerce systems with existing enterprise systems and the lack of internationally recognized standards covering such activities as transaction processing, security and authentication were also identified. Networking bandwidth was a prominent concern among developing countries, many of who are still developing basic telecommunications infrastructures
- ❑ **Workforce Issues** There was a strong consensus among WITSA members that people issues will play an important part in the development of electronic commerce. The shortage of skilled workers, a perennial problem for the IT industry, is the most important issue for the majority of respondents. The leadership of business executives was also called in question with a significant proportion of WITSA members believing that those who run enterprises are too averse to taking risks. Training and the cost of employing skilled workers were also high on the agenda, although there were some members who did not see the workforce as a stumbling block at all to the growth of electronic commerce.
- ❑ **Public Policy** As industry associations, WITSA members are closely involved in influencing public policy in their countries. Leading public policy issues highlighted by respondents included the development of standards for authentication that would ensure trading partners are legitimate; the impact on electronic commerce of the taxation of online sales and the confusion caused by conflicting international contractual and legal frameworks. Respondents also pointed to limits on the use of encryption by governments concerned about national security and crime fighting. The ability of governments to influence the growth of electronic commerce is underlined by the fact that over 70% of WITSA members say public policy is critical to the growth of electronic commerce.
- ❑ **Taxation** Although taxation scores highly in the public policy arena, overall it is perceived as less of a barrier than any other issue related to electronic commerce. Local sales taxes are perceived as most harmful to electronic commerce. Despite a lack of clarity on taxation in many countries, the majority view was that taxes were not an important barrier to electronic commerce.

- ❑ **Business Processes** While new Internet only businesses such as auction sites and share dealing services have been launched, the majority of organizations trading on the Internet are established businesses that must integrate their electronic activity with existing business processes. The biggest problem, identified by the survey, is a fear of opening corporate systems to outsiders: both customers and suppliers. WITSA members also pointed to a lack of business models for newcomers to adopt. Respondents also identified the logistical challenges of the real time environment of electronic commerce and the need to be sure of quality business results from electronic information exchanges.
- ❑ **Costs** In line with the emphasis on people issues, the most significant costs for those implementing electronic commerce are connected with organizational change. The costs of changing business processes and adapting corporate cultures to accommodate electronic commerce are seen to represent the biggest cost elements. Adapting existing systems, running dual systems, building new systems and buying new products and services are seen as less significant. This finding reflects the fact that the cost of technology and of the skills to implement it are beginning to decline as electronic commerce features are incorporated in existing products and as skills become more widely available.
- ❑ **Consumer Attitudes** The experiences of WITSA member companies in convincing customers to adopt electronic commerce again underlines the need to reassure users that they can trust the Internet. Fear of committing personal information such as credit card numbers, addresses and telephone numbers to cyberspace was mentioned most often by WITSA members as a significant objection from customers. Fear of losing money by purchasing goods from unknown companies and the absence of regulation governing procedures in the event of disputes were also important reasons for being wary of electronic commerce.

IV. PRIVACY

Effective means must be in place to assure individuals and businesses that rights to privacy and information security will be upheld, and to that end WITSA supports measures, such as the adoption of industry codes, to afford reasonable and appropriate levels of privacy protection and information security, and to clear avenues of redress. WITSA believes that industry and consumers should, as much as possible, be left to regulate themselves through the marketplace of competing information services featuring various levels of information security at a range of costs. The current marketplace is rapidly developing and promoting commercial products to provide businesses and consumers with proactive competitive choices and flexible tools to protect individual privacy online. In addition, competing third-party entities are emerging to ensure compliance by verifying web site integrity with respect to adherence to established privacy guidelines. WITSA supports the development of reliable third-party entities which organizations can engage to verify that they are adhering to their own set of privacy principles and practices.

a. WITSA Statement on Privacy:

A WITSA [Statement](#) on Privacy, released in August 1998, outlined the following Key elements of Effective Privacy Protections:

Individual Privacy Protection:

- ❑ **Choice:** Provide individuals with choice to opt-out of personal data collection and use and opt-out of disclosure to third parties. Any exceptions to these opt-out provisions must be clearly described.
- ❑ **Access / Accuracy:** Provide appropriate mechanisms to allow individuals to control the access (to read, write, modify and use) their personal data and to review and correct personal data.
- ❑ **Authorization :** Provide mechanisms to allow individuals to grant control to access their personal data and to modify it.
- ❑ **Authentication :** provide appropriate mechanisms to allow individuals to authenticate who they are before giving access to their personal data.
- ❑ **Recourse:** Provide individuals with clear means for redressing possible violations of an organization's stated privacy principles and practices.

Organizational Responsibility:

- ❑ **Notice / Awareness:** Provide clear information on policy for collection, use, and disclosure of personal data.

- ❑ **Disclosure:** Work actively to ensure that individual data are disclosed only to third parties that have implemented business practices to protect privacy.
- ❑ **Collection:** Limit collection and use of personal data to that which is appropriate and needed.
- ❑ **Protection :** Keep personal data secure from being tampered with and from being changed without permission.
- ❑ **Security:** Keep personal data secure from unauthorized access, disclosure and use.

Enforcement Mechanisms:

- ❑ **Accountability / Oversight:** Establish systems for individuals to seek resolution or redress of possible violations of stated privacy principles and practices.
- ❑ **Enforcement:** Support strong enforcement of existing legal and regulatory remedies.

V. INFORMATION SECURITY

Aggressors attack at the point of maximum leverage. For modern society, this means critical infrastructure—transportation, telecommunications, oil and gas distribution, emergency services, water, electric power, finance and government operations. Increasingly, a critical information infrastructure supports these vital delivery systems and becomes itself a target of opportunity for terrorists, adversary nations, criminal organizations, and non-state actors. This potential vulnerability raises numerous difficult questions for industry and international, national, and local governments about how to best provide critical information protection. Both government and industry have a major stake in protecting critical infrastructure and its underlying information resources from intentional attack or natural disaster. The approach taken in addressing issues of critical information infrastructure reliability and security must highlight that policies necessary for the development of electronic commerce be industry led, market driven, voluntary and self-regulatory.

a. Global Information Security Summit & Working Groups

In order to raise awareness of issues, promote cross-national and cross-sector collaboration, identify policy needs, highlight information security best practices and partnership initiatives, WITSA on October 17-17, 2000 launched the inaugural **Global Information Security Summit** in Washington, D.C. The Summit also launched the **Partnership for Global Information Security (PGIS)** - a partnership between industry and government leaders from around the world to address critical communications and information sharing issues surrounding information security in a digital economy: Best Practices, Workforce, Research & Development, Cyber-crime & Law Enforcement, and Public Policy & Legal. A [Second](#) Summit will be held in Belfast on May 31 to June 1, 2001. A Third Summit will be held in North America in late 2001.

b. Statement on the Council of Europe Draft Convention on Cyber-Crime:

On November 30, 2000, WITSA issued a [Statement](#) on the Council of Europe Draft Convention on Cyber-Crime to [COE](#) General Secretary Walter Schwimmer, voicing concerns over the latest revision of the draft COE [Convention](#) on Cyber-Crime, but supported the objectives of improving international law enforcement cooperation and mutual legal assistance to keep pace with the increasingly international environment. This legally-binding text would be the first international treaty to address criminal law and procedural aspects of various types of offending behavior directed against computer systems, networks or data, and aims to harmonize national legislation in this field, facilitate investigations and improve co-operation between the authorities of the 41 member states. In the statement, WITSA expressed serious concerns with several of the provisions contained in the draft cyber-crime convention. The draft convention may impose burdensome data preservation requirements on Internet service providers (ISPs); make ISPs liable for third party actions; and restrict legitimate activities on the Internet.

c. Global Security Project

In December 2000, WITSA collaborated with McConnell International LLP in a first-of-its-kind International Security Law Project, aiming to identify the measures taken by the governments in 52 countries across the world to combat information security. The report, entitled "Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information", was published on December 7, 2000 and is available [online](#). A joint December 7, 2000 WITSA/McConnell International press release is also [available](#).

as well as a [January 2, 2001](#) press release regarding updated references to Canadian cyber crime legislation.

The report looked at ten different types of cyber crime in four categories: data-related crimes, including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery. Among some of the key findings: Thirty-three of the countries surveyed have not yet updated their laws to address any type of cyber crime. Of the remaining countries, ten have enacted legislation to address five or fewer types of cyber crime, and nine have updated their laws to prosecute against six or more of the ten types. Of those countries, only one, the Philippines, indicated that updated legislation is currently in place to prosecute a future perpetrator of all of types of crimes. In addition to highlighting the efforts of 19 countries that have partially or fully updated their criminal laws, the report also identifies efforts underway in 17 countries that have not updated their laws, including Cuba, Latvia, New Zealand, and Zambia.

d. WITSA Identifies Cyber Security as a Top Priority

A February 2000 WITSA [survey](#) of WITSA member IT industry association executives identified cyber security as the next “top priority” issue facing the IT industry around the globe. While association executives expressed a high degree of personal awareness of the InfoSec issue, four out of ten said customers in their countries are either “not very” or are “unaware” of computer protection matters. Sixty-five percent of respondents said their national or regional governments have strong awareness in this area. While 94 percent of the trade association executives personally view InfoSec a top priority issue, this number dropped to 82 percent in reference to their member companies, 65 percent to their governments and 41 percent to end users. Seventy-six percent of respondents say they are meeting with their respective governments to raise awareness of InfoSec issues; almost 60 percent said their governments are seeking meetings with industry on the same issue.

e. Information Security Framework Statement:

In developing industry positions on national CIP issues, WITSA published the [statement](#), “*Critical Information Protection (CIP): A Framework for Government / Industry Dialogue* (June 1999), and established an initial list of general principles which reflect the opinion of its membership and which serves as a guide for the development of future policy.

Scope:

- ❑ The protection of the national information infrastructure must be based upon a minimum amount of government (national, provincial, and local) regulation.
- ❑ The cost of protecting the national information infrastructure must be kept to the lowest level possible commensurate with the threat and the consequences of attack. Parties must be able to differentiate between potential vulnerabilities and specific threats.

Roles and Responsibilities:

- ❑ Industry builds and operates the Global Information Infrastructure and, as such, has primary responsibility for CIP requirements, design and implementation.
- ❑ Industry and governments share an interest in the proliferation of a free and open Internet, electronic commerce, other value-added networks, and an efficient, effective information infrastructure generally.
- ❑ In protecting these resources, the specific and immediate priorities of governments and industry may diverge. Specific and immediate priorities will need to be balanced against longer-term priorities.
- ❑ Industry will be guided by business considerations to protect itself against physical and cyber attack as the threat to the information infrastructure evolves.
- ❑ Where CIP action is required to protect the public good, governments must identify such instances and create appropriate public funding mechanisms to support the public good.

Globalization:

- ❑ The Internet and electronic commerce are inherently global in nature; therefore, critical information protection will require collaboration among international bodies.

- ❑ Governments are Urged to establish and maintain channels of communication with private and public entities having infrastructure assurance interest in the sector; and to
- ❑ Establish and operate an effective information-sharing program, including opportunities for anonymous information sharing.

Communication and Coordination:

- ❑ Positive interaction between governments and industry is essential. Among issues which will require on-going communication and assessment is the need to balance the right to privacy with national security concerns.
- ❑ Industry must monitor the private sector portion of the national information infrastructure and cooperate both internally and with governments in reporting and exchanging information concerning threats, attacks, and protective measures. Coordination among principals must facilitate creation of early warning systems.

Legal Frameworks:

- ❑ In creating the information infrastructure, as well as attendant tools and technologies, industry must be provided safe harbor protections and its works viewed as incidental to losses caused by criminal or malicious misbehavior or natural disasters. National law should provide such protection regardless of an attack's origin.
- ❑ Distinctions must be made among cyber-mischief, cyber-crime and cyber-war to clarify jurisdictional issues and determine appropriate responses. The adequacy of current laws to prevent these threats must be reviewed.
- ❑ Existing laws must be adapted as necessary to allow appropriate levels of information-sharing among companies.
- ❑ Government policy in areas such as research and experimentation tax credit and software encryption must be reviewed in light of common CIP goals and objectives.

Education:

- ❑ National law enforcement agencies must gain sufficient cyber-crime expertise to combat specific threats and to investigate specific criminal acts.
- ❑ Emergency response organizations must gain sufficient disaster recovery expertise to minimize the effect of catastrophic events on the information infrastructure.

f. Statement on Government and Law Enforcement Access to Transmitted Information In the Digital Environment

In the era of voice telephony, there was general agreement around the world that governments and law enforcement agencies could have legal access to telephone conversations for legitimate security and law enforcement activities. This principle is now being questioned, however, as the world is becoming increasingly digitized, and access to transmitted information includes not only voice telephony, but also data and video information. The tendency simply to extend voice telephony access to other media is becoming increasingly problematic to the business community in the global environment. In a [*Statement on Government and Law Enforcement Access to Transmitted Information In the Digital Environment*](#) (August 1998), WITSA endorsed the following principles concerning legal access to information in the networked environment, which are consistent with those being developed by a number of other international business organizations:

- ❑ Users should be free to choose the type and strength of encryption they feel is necessary to protect their information.
- ❑ Legal access by any given jurisdiction shall only be to information actually stored in that jurisdiction at the time of proper judicial notification.
- ❑ A business shall have no obligation to maintain the means to provide clear text of transmitted information, including e-mail, unless the information is stored on the business's facilities in a non-

transitory manner at the time the information is properly requested and during the period of the proper legal request, and is accessible in clear text by the business.

- ❑ Legal access requests should be specific, and limited in scope and duration.
- ❑ There should be no requirement that encryption keys be filed or registered with any third party, either public or private.
- ❑ In order to protect personal privacy, all personal information that is accessed for any reason must be protected by the accessing agency.
- ❑ All information that has been accessed must be returned once legal proceedings are complete, and any copies of such information should be destroyed.

VI. IT WORKFORCE ISSUES

The Internet and IT have become the twin pistons of the economy in countries across the world. The demand for IT workers is large and growing. The greatest need for IT workers typically is in the largest segment of the economy--smaller non-IT firms. While Non-IT companies have more aggregate demand, the average IT company has far more jobs to fill.

WITSA believes workforce related barriers constitute a growing predicament to the growth of IT and the high-tech industry. WITSA has undertaken an "inventory" of existing studies, reports and surveys conducted in the respective WITSA countries, which is thought useful to obtain a thorough overview about what was being done on this critical issue across the world. The findings will provide a useful tool to establish best practices, recommendations and other remedies to the barriers caused by the growing skills gap.

VII. TAXATION AND TARIFFS IN AN E-COMMERCE ENVIRONMENT

Many taxation issues are not new or unique to electronic commerce but have already developed in conventional commerce, which increasingly relies on new modes of communications and increasingly crosses national borders. The mode of doing business through electronic commerce may add new layers of difficulty and may require solutions to both the problem of no taxation or double taxation and to the problem of administrative burden.

Simplicity, clarity, and fairness must be promoted in both national tax regimes and supranational tax regimes (e.g. the European Union's value-added tax system), as well as bilateral tax agreements for the avoidance of double taxation based on international models, in order to allow for the global trading potential of electronic commerce. Tax rules everywhere should be understandable and user-friendly to allow for the potential increase in cross-border sales by companies. Application of existing taxation principles to the electronic medium must also be built upon tools that businesses already use or are required to develop to meet their market needs. Tax obligations should especially fit into the new streamlined processes found in electronic commerce. It is only in this way that high tax compliance can be sustained with the least burden and the fewest economic distortions.

Differing rules on the application of indirect taxes may have a more adverse effect on e-commerce than direct taxation – such as income taxes. Burdensome and costly tax withholding requirements and the threat of double taxation are caused by current inconsistencies between governments on definitions, classification, levy, assessment, and collection. In addition, there should be no discriminatory government taxes, charges or fees on electronic commerce transactions. Transactions conducted using electronic commerce should receive neutral tax treatment in comparison to transactions using non-electronic means. Internet specific taxes will stifle the development of on-line business

WITSA is of the opinion that a global perspective is required when addressing this subject, as electronic commerce cuts across national boundaries to a greater degree than traditional forms of business. Therefore, consistent taxation approaches at the international level are absolutely critical to ensure the effectiveness of tax treatment in the digital economy and the avoidance of double taxation.

a. Consumption Taxes & E-Commerce

Consumption taxes are intended to be borne by consumers, with sellers acting merely as tax collectors. If not properly designed, however, sales taxes may impose an economic burden on business. Sellers bear the cost of determining the applicable tax rate, which may depend on the type of product and the location and type of customer; preparing invoices according to tax rules; collecting tax; filing and remitting tax; and maintaining tax records. If tax is assessed incorrectly, the seller (or its third-party agent) typically will be held responsible for any shortfall and will not be able to reclaim it from the customer. In addition, cross-border transactions raise the possibility of double taxation, which can create a significant competitive disadvantage.

The avoidance of double taxation should be the first and foremost among the general principles governing consumption taxation, because the prospect of double taxation will do more to inhibit the development of electronic commerce than any other tax factor.

Significant attention should be given to simplification of indirect taxation. The current inconsistencies among definitions, classification, treatment of combined or bundled services, source of supply rules, registration requirements, invoicing requirements, payment procedures, reporting, record retention, reverse charges, levy, assessment, and collection (including VAT withholding obligations of the customer) are widely cited by businesses of all sizes as a significant burden on international commerce.

At the time of the 1998 OECD Ministerial meeting on electronic commerce, it was proposed that the OECD form Technical Advisory Groups (TAGs) to assist in taking forward the work on taxation and electronic commerce. Five TAGs were established in January 1999 for two years to allow them time for a thorough consideration of all the issues. The Consumption Tax TAG is examining consumption taxes and electronic commerce in the following areas:

- ❑ rules for the consumption taxation of cross-border trade should result in taxation in the jurisdiction where consumption takes place and an international consensus should be sought on the circumstances under which supplies are held to be consumed in a jurisdiction;
- ❑ for the purpose of consumption taxes, the supply of digitized products should not be treated as a supply of goods;
- ❑ where business and other organizations within a country acquire services and intangible property from suppliers outside the country, countries should examine the use of reverse charge, self-assessment or other equivalent mechanisms where this would give immediate protection of their revenue base and of the competitiveness of domestic suppliers; and
- ❑ countries should ensure that appropriate systems are developed in co-operation with the World Customs Organization and in consultation with carriers and other interested parties to collect tax on the importation of physical goods and that such systems do not unduly impede revenue collection and the efficient delivery of products to consumers.

WITSA is currently considering a statement addressing specific issues raised by the OECD review of consumption taxation and e-commerce

b. VAT Exemptions

VAT exemption for industries and firms inhibits the use of outsourcing for information technology services by creating a price differential between the cost of contracting and performing services in-house. This, in turn, provides a disincentive for such firms to seek outside expertise and negatively impacts their competitiveness in the global marketplace. As outlined in its [*Statement on the Impact of VAT Exemption on IT Outsourcing*](#) (September 1999), the most notable example of this situation is the financial services industry in Europe, though other countries have raised the issue as well. Since the global IT market in financial services exceeds US \$200 Billion, any disincentive for outsourcing is significant. Governments wishing to provide the effect of tax exemption to particular industries or firms have a number of options:

- a) They could “zero rate” them with respect to VAT. Under this scenario, the institution would charge VAT to customers at a zero rate but, therefore, be technically capable of recovering VAT paid to suppliers;

- b) Depending on the nature of the VAT regime, the provisions of IT services could be deemed to be an acquisition for a “credible purpose”, for VAT exempt organizations. This would enable the organizations to reclaim any VAT paid on the acquisition of IT services;
- c) In the case of financial services, they could require financial institutions to charge VAT on service fees, such as transaction fees, loan fees and so on. This would enable the financial institutions to reclaim all or part of the VAT paid on its inputs such as IT services.

Governments should as far as possible avoid taxation arrangements which distort commercial business decisions and adopt one of the options described above and in the WITSA statement in their treatment of VAT exempt industries.

c. Lowering Trade Barriers, Including Tariffs, Encourages Global Electronic Commerce. The World Trade Organization's (WTO) Temporary Commitment To The Duty Free Treatment Of Electronic Transmissions Should Move To A Permanent One

An important goal of the business community is to promote the expansion of electronic commerce and to prevent the creation of trade barriers in the form of burdensome customs duties or tariffs on services and products delivered electronically. Lowering trade barriers, including tariffs, is one of the most obvious means of encouraging international trade as well as global electronic commerce.

For 50 years, countries have been moving in the direction of an international trading system as free as possible of trade barriers in the form of burdensome customs duties or tariffs on goods and services, regardless of the method of delivery. Commitments in this area make the business environment stable and predictable and give business a clearer view of their future trade opportunities. With stability and predictability as part of the multilateral trading system, trade increases, investment is encouraged, jobs are created, and consumers can enjoy the benefits of competition -- choice and lower prices.

WITSA worked with our international business associations in supporting the Alliance for Global Business (AGB) Statement on the “ Duty-Free Treatment of Electronic Transmissions and Its Importance to Global Electronic Commerce and Expanded International Trade .”

VIII. E-GOVERNMENT

The information revolution has pushed companies to change and adapt to new technologies, competitors, and business models with consumers now expecting better service and competitive pricing. The information revolution is reaching government. Both businesses and consumers are asking more from government in terms of services, business practices, and cost-savings. The government has been challenged to keep pace with these rapid technological innovations and demands. Slowly, governments are coming online and providing better services while exploring new ways to interact with both citizens and businesses. Streamlining government operations by moving services onto the Web will save significant taxpayer money and provide better services to citizens.

E-Government Challenges

Despite all the obvious benefits of bringing government services and activities online, the effort will face at least two challenges -- security and privacy. Because of the sensitive nature of the information that is stored in government databases, both system security and information privacy will be important issues. If transactions such as online license registration or tax payments are to gain the trust of both citizens and public employees, the security of these transactions must be guaranteed. In addition, any government pursuing e-government policies will be challenged to ensure that these services are accessible by all citizens.

WITSA will be preparing a statement on this topic in the near future.

IX. INTERNATIONAL TRADE NEGOTIATIONS

WITSA recognizes the World Trade Organization ([WTO](#)) as the international body dealing with the rules of trade between nations. WTO agreements provide the legal ground-rules for international commerce and

for trade policy. These multilateral agreements have three main objectives: to help trade flow as freely as possible, to achieve further liberalization gradually through negotiation, and to set up an impartial means of settling disputes. A number of simple, fundamental principles run throughout all the WTO agreements: non-discrimination ("most-favored-nation" treatment and "national" treatment), freer trade, predictable policies, and encouraging fair competition. With stability and predictability, the multilateral trading system should encourage trade and investment flows, create jobs, and provide consumers the benefits of competition - expanded choice and lower prices.

WITSA strongly supports WTO and its objectives in creating an open trading system free of barriers. WITSA is committed to maintaining open markets, reducing protectionism and sustaining the momentum of liberalization achieved by the General Agreement on Tariffs and Trade (GATT)/WTO over the last forty years. WITSA supports the launch of a new round of multilateral trade negotiations, which would provide an opportunity to embark on further liberalization of barriers to international trade, including trade in information technology goods and services. WITSA also recognizes and support the WTO work [program](#) on electronic commerce, which since its inception in 1998 has included a thorough examination of issues related to electronic by the Goods, Services and TRIPS (intellectual property) Councils, and the Trade and Development Committee.

a. Priorities for a New Round of Multilateral Trade Negotiations

The WITSA [Statement](#) on the Third WTO Ministerial Conference (September 1999), outlines industry's highest priorities regarding the next round of multilateral trade negotiations:

- ❑ **Services: The "Built-In Agenda":** WITSA urges trade ministers to launch a new Round of trade negotiations, with a focus on liberalizing trade in services in a host of sectors including the information technology services sector: (1) A new Round should achieve much broader coverage of services sectors through new or improved national schedules of commitments that go beyond the standstill agreements which characterize many of the Uruguay Round commitments; (2) Ministers should closely monitor ratification and implementation of both sector agreements already signed and new agreements negotiated in the new Trade Round; and (3) countries seeking accession to the WTO should make strong commitments to services liberalization.
- ❑ **Information Technology Services:** The 2000 Services Round should work to insure that global markets for information technology services remain open and free of burdensome oversight and regulation. As important as direct negotiation in information services is, equally important is the negotiation of substantial liberalization in the service sectors served by information technology services.
- ❑ **Implementation and Expansion of Existing Commitments:**
 - **Agreement on Basic Telecommunications:** WITSA calls on trade ministers to (1) fully implement the historic 1997 Agreement on Basic Telecommunications Services, including the pro-competitive regulatory principles contained in the Reference Paper; (2) Work to obtain meaningful market opening commitments from those countries that have yet to schedule commitments on basic telecommunications; and (3) Expand commitments from those countries that made less than full market-opening commitments. See also the WITSA [Statement](#) on the WTO Basic Telecommunications Services Negotiations (February 1997) and the [Resolution](#) to Support Telecommunications Commitment by Countries Seeking Accession to the WTO (September 1997).
 - **TRIPs Agreement:** Ministers should call for the prompt and full implementation of commitments undertaken by WTO members under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs). Compliance with deadlines should not be reopened in future negotiations.
 - **Information Technology Agreement (ITA):** Ministers should call for the full implementation of the historic 1997 Information Technology Agreement and encourage those countries which have not scheduled commitments to do so.
 - **Transparency Agreement:** A binding transparency agreement would establish global norms for the open conduct of procurement by governments. WTO Ministers should call on Member Countries to (1) participate in active negotiations at the WTO leading to completion of a binding

agreement on transparency in government procurement at the Seattle Ministerial in 1999; (2) achieve early ratification and implementation of the agreement; and (3) involve private sector representatives in the development of a regulatory framework for implementation. See also the WITSA [Statement on WTO Negotiations on Transparency in Government Procurement](#) (1999).

- **Movement of Key Personnel:** WITSA urges WTO Ministers to identify as a priority for the new GATS round the negotiation of the reduction of government measures that impede or prevent the timely movement of business persons on a temporary basis among WTO members, including: (1) All GATS signatories should agree on common terms for executives, managers and specialists under intra-company transfers; (2) the establishment of a multilateral framework of principles and rules for facilitating the temporary movement of international assignees; and (3) a procedure whereby WTO members offer specific commitments with respect to their statutes, policies and procedures affecting the temporary movement of international business personnel.

b. WTO and E-Commerce

Electronic commerce is not a new form of trade but rather a new medium/ mode for conducting trade in goods and services. All forms of electronic commerce, as traditional commerce, can be categorized into either the goods or services category and therefore specific agreements governing trade in goods, trade in services, or trade-related intellectual property apply. Recognizing the many contributions electronic commerce is making to the expansion of international trade, WITSA members in the [Statement on WTO and Electronic Commerce](#) (September 1999) call on WTO to:

- ❑ Make permanent and binding the May 20, 1998 **Moratorium on Customs Duties** on Electronic Transmissions;
- ❑ Affirm the importance of the **basic telecommunications infrastructure** to the growth and development of electronic commerce and urge countries to further liberalize these markets;
- ❑ Reaffirm that existing WTO obligations, rules, disciplines and commitments, including the GATS, GATT and TRIPS agreements are **technology neutral**;
- ❑ Agree that governments should refrain from enacting any **new and unnecessary measures** that would impede the growth of international electronic commerce;
- ❑ Refrain from enacting trade-related measures that have the **effect of impeding**, actually or potentially, international e-commerce, even if enactment of such measures would not otherwise violate existing international legal obligations;
- ❑ Agree that **measures affecting e-commerce must be consistent** with the following fundamental principles of international trade law:
 - National treatment and non-discrimination
 - Most Favored Nation (MFN) treatment
 - Transparency
 - Notification, review and consultation
- ❑ Work within the General Agreement on Tariffs and Trade (GATT), General Agreement on Trade in Services (GATS) and the Agreement on Trade-related Aspects of Intellectual Property Protection (TRIPS) to **identify, reduce or eliminate barriers** to international e-commerce
- ❑ Agree that there may be certain e-commerce related **issues that are not appropriate** subjects of international trade obligations and/or within the current scope of trade policy.
- ❑ Refrain from **prematurely classifying** all electronic transactions as good or services, but direct relevant WTO working bodies, in cooperation with private sector experts, to thoroughly examine the implications of classification;
- ❑ Recognize that the development of electronic commerce depends on cross-border transactions in all industry sectors and urge negotiators to **liberalize cross-border services** during the negotiations.

X. SEIZING DIGITAL OPPORTUNITIES

Preventing a "digital divide" is an essential goal for both business and governments. According to the bench-mark WITSA study, [The Digital Planet](#), one socioeconomic discontinuity remains a major world challenge: the top ten information economies represent 80 percent of the global ICT market; the bottom ten (of 52 surveyed countries) represented a collective share of less than one percent. This disparity has come to be known as the "Digital Divide" – the gap between nations that can and cannot afford technology investments. Business has been working hard through independent projects to provide assistance to disadvantaged economic groups, localities, regions or countries, aimed at transforming the digital divide into a digital opportunity. Almost any sizeable company today has taken up some local or regional responsibility in bridging the digital divide. Developing countries can reap these benefits resulting from the technological innovations that have led to the commercialization of the Internet -- they can leapfrog technologies and become active participants in the online global economy. However, these assistance programs will become a digital opportunity only if governments adopt a policy framework which ensures that access to digital information and communication networks is a viable option for the citizenry at large.

a. Statement on Digital Opportunities

In a January 2001 [statement](#) entitled "*Seizing Digital Opportunities: A Business Perspective*", published in conjunction with its Alliance for Global Business (AGB) partners, WITSA outlined its belief that such a policy framework is one that promotes open markets, competition and private sector investment. Incentives also have to be correct for skill acquisition and necessary changes in the organization of the workforce, and governments must pursue important trade-related objectives enabling innovation, including:

- An early focus and agreement on the agenda for a new WTO Round;
- Substantial outreach to LDCs to encourage their full participation;
- Reinforced and implemented commitments;
- An acceleration of the Services 2000 effort;
- The strengthening of intellectual property protection;
- The elimination of tariff inhibitions to products essential for ICT;
- The permanence of tariff-free cyberspace;
- Serious attention to trade facilitation and full implementation of the Valuation Agreement;
- Elimination of non-tariff barriers;
- Implementation of international standards and simplified conformance testing; and
- Expeditious accession of new members to the WTO.

b. Business-Government Forum on Digital Opportunity

In conjunction with the OECD "[Emerging Market Economy Forum](#)" in Dubai on January 16-17, 2001, WITSA also hosted with its AGB partners, a January 15 [business-government forum](#) on e-commerce entitled "Maximizing the Digital Opportunity". The purpose of the business-government forum was to highlight the private sector's priority needs for policy coherence between countries, and the international trade and economic policy issues "which need to be addressed to make the digital economy a reality for emerging market economies as well as advanced market economies" (see [press release](#)). Several WITSA representatives presented at the two Dubai events, including:

- **Ms. Kimberley Claman**, WITSA Executive Director (see presentation at [OECD](#) or [WITSA](#) site)
- **Dr. Waclaw Iszkowski**, President of the Polish Chamber of Information Technology and Telecommunications ([PIIT](#))
- **Ms. Silvia Bidart**, Executive Director of Cámara de Empresas de Software y Servicios Informáticos; [CESSI](#) (Argentina); and Chairman of the WITSA Task Force on Developing Countries. See presentation at [OECD](#) or [WITSA](#) site.

c. E-Readiness Report

Separately, WITSA collaborated with McConnell International in issuing a first E-Readiness [report](#), entitled "*Risk E-Business: Seizing the Opportunity of Global E-Readiness*" (August 2000). The Report measures the E-Readiness in 42 countries, that is the capacity to participate in the global digital economy.

According to the report, the current ICT-led expansion is at risk, threatening the global economy. Global e-society stands at a turning point. Action or inaction by national governments and industry leaders will produce a very mixed set of outcomes. Some countries will make technology a driver for a new national economy, leaping from an agrarian or industrial base into the knowledge economy. Others will fail to take the necessary steps and will be left behind in the race for cyber markets. The 42 countries were selected as “critical economies” because they represent the “source of the next phase of world economic growth”: make up almost 75 percent of the world population and a quarter of the global GDP. Twenty-three of the 42 countries have at least two areas where substantial improvement is needed. Without significant progress over the next three years, these countries will face great challenges in catching up with the global leaders. The level of readiness was based on criteria such as Internet access, E-leadership, information security, human capital, and E-business climate.

XI. INTERNET GOVERNANCE

As a non-profit corporation formed in September 1998 to oversee Internet technical management functions previously managed by the U.S. government, the Internet Corporation for Assigned Names and Numbers (ICANN) has assumed a number of responsibilities in technical management of protocols, addressing and domain names, which are critical to the stability and growth of the Internet. ICANN is an unprecedented effort by Internet business, technical, non-commercial and academic communities to create a consensus-based, globally representative non-governmental policymaking entity. In the two plus years since its creation, ICANN has celebrated many achievements and still has many hurdles to overcome. Its adoption of an arbitration system in late 1999 has proved to be an effective tool against cyber-squatters; its online election of five Board Directors by an at-large membership from around the world has demonstrated its commitment to inclusion and transparency. Its recently adopted program for adopting new generic top-level domain names (gTLDs) has offered a no-nonsense approach to enable expansion of the names space of the Internet without jeopardizing its stability or functionality.

WITSA was an active supporter of the establishment of ICANN and was a co-sponsor of the Barcelona-Monterrey-Washington 1999 proposal that led to the formation of one of its constituent groups, the Domain Names Supporting Organization (DNSO). WITSA is an active member of the DNSO Business Constituency group as are twelve of its national member IT industry associations. WITSA and its member associations helped elect the three business representatives to the current Names Council (NC) -DNSO’s executive body.

Statement of Support for the Internet Corporation for Assigned Names and Numbers (ICANN)

In its [Statement of Support for the Internet Corporation for Assigned Names and Numbers \(ICANN\)](#) (November 2000), WITSA appealed to all Internet stakeholders, whether from the Internet business, technical, non-commercial or academic communities, to appreciate the importance of working constructively together with the common goal of empowering ICANN and its constituent organizations to complete the privatization of the Internet technical-management functions. WITSA supports the following key principles related to the technical management of the Internet:

- ❑ **Strong Private sector leadership:** WITSA recognizes that ICANN has actively collaborated with Internet stakeholders in building three supporting organizations with separate responsibilities.
- ❑ **Effective arbitration against “bad faith” domain name registrations:** WITSA strongly supports the Uniform Domain Name Dispute Resolution Policy (UDRP) against “bad faith” generic top level domain name (gTLD) registrations, such as .com., .net., and .org as an option to national law, and as a low-cost and effective mechanism for dealing with conflicts related to protecting the rights of intellectual property in the domain name space. WITSA also welcomes the initiative recently announced by WIPO to develop arbitration guidelines against bad faith gTLD registrations not based on registered trademarks.
- ❑ **Effective Competition among Registrars:** WITSA supports ICANN’s registrar accreditation policy for the .com, .net, and .org top-level domains, which has enabled robust competition among more than 100 registrars, while maintaining the stability of top-level domains. The registrar accreditation policies should be extended to all new registrars for any new gTLDs.

- ❑ **Broad Participation in Policy Formulation and Procedures:** In undertaking the technical management of the Internet, ICANN must balance the broad, bottom-up participation of Internet constituents in policy making with the need to make timely resolutions vital to the safe and stable operation of the Internet. WITSA encourages all private sector Internet stakeholders to work with ICANN in continuing to improve its participatory processes with the goal of achieving timely resolution of policy issues with the participation of affected parties.
- ❑ **Transparency:** WITSA believes a private sector led, consensus-driven system for technical Internet management must include transparent procedures for policy formulation and dissemination of information to the public. Private sector Internet stakeholders are encouraged to work with ICANN constructively in identifying further areas of improvement as regards openness and transparency.
- ❑ **Effective Review Process:** WITSA supports ICANN's efforts to implement effectively procedures to address complaints of undue harm to members of the Internet constituency and regarding possible breaches of its mandate, as stipulated in its Bylaws and Articles of Incorporation (e.g. the *Reconsideration Process*, the *Independent Review Policy*, and *Arbitration Process*).
- ❑ **Membership Mechanisms, Accountability and Representation:** ICANN is to be applauded for the completion of the 2000 election of five At-Large Directors for the ICANN Board, providing Internet stake holders from all corners of the world with historically unprecedented representation in the decision making process affecting the technical management of the Internet. WITSA further welcomes the launch of a comprehensive study of the concept, structure and processes relating to the At-Large membership in view of ICANN's mission and structure.
- ❑ **Introduction of New gTLDs:** WITSA recognizes the need for new generic Top-Level Domain Names (gTLDs) on the Internet root server system, and supports ICANN's cautiously established procedures for approving these. Key considerations are maintaining the Internet's stability, enhancing competition for registration services, enhancing the utility of the domain name system (DNS), and ensuring appropriate protections of rights of others in connection with the operation of new TLDs.
- ❑ **Enhancing the security and operation of the root-server system:** WITSA supports the plan adopted by ICANN on July 15, 2000, and as developed by the DNS Root Server System Advisory Committee (RSSAC), to enhance the security and operation of the root-server system.
- ❑ **Sound Financial Footing:** WITSA will continue to support ICANN's important work in the domain name field, and encourages ICANN to seek a broad-based funding platform. The domain name system affects a vast number of users, which should mean stakeholders should ultimately cover the necessary expenses related to its operation and management.

-END-