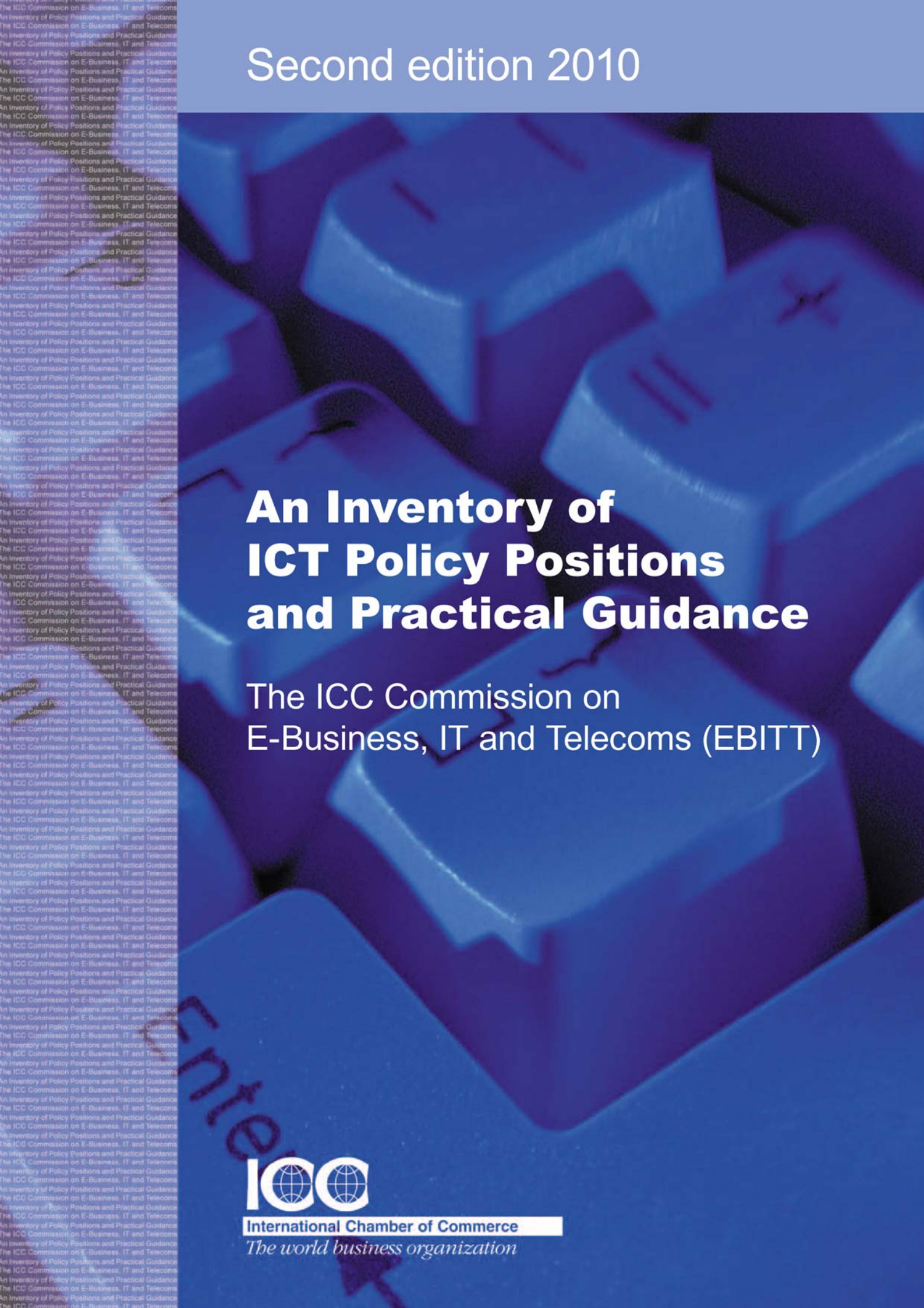
Second edition 2010

An Inventory of ICT Policy Positions and Practical Guidance

The ICC Commission on E-Business, IT and Telecoms (EBITT)



International Chamber of Commerce
The world business organization

Copyright © 2010
International Chamber of Commerce

All rights reserved. No part of this work may be reproduced or copied in any form or by any means – graphic, electronic, or mechanical, including photocopying, scanning, recording, taping, or information retrieval systems – without the written permission of International Chamber of Commerce (ICC), Paris.

Contact:

Ayesha Hassan
Senior Policy Manager, E-Business, IT and Telecoms
Executive in charge of Information and Communication Technologies (ICT) Policy

International Chamber of Commerce (ICC)
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 28 59
Email ebitt@iccwbo.org
Website www.iccwbo.org

Foreword

We are pleased to present the updated second edition of this inventory of policy positions and practice guidelines on a range of issues from the work of ICC's Commission on E-Business, IT and Telecoms (EBITT) and its task forces. This inventory provides comprehensive information about the substantive positions and recommendations of ICC's experts on many public policy issues relevant to the Internet and Information & Communications Technologies (ICTs) and all business sectors.

ICC is the global focal point for our members from around the world to develop policy positions and practice tools for policy decision-makers, business users, and all users. The EBITT Commission members from all geographies and sectors have pooled their experiences and perspectives to develop the consensus-built positions and recommendations contained in this inventory. The recommendations are based on extensive consultation among business experts. ICC policy documents go through a rigorous vetting by ICC national committees and members in 120 countries, and thus reflect a wide range of business opinion.

Having the right policy framework in place to maximize the potential of these technologies and mediums as engines of economic growth and social development is essential for business and all users. Governments, business, civil society, technical community representatives and international organizations share a common goal which is to bring the benefits of the Internet and ICTs to more people around the world. The joint efforts of all and the exchange of information and good practices are essential.

With the second edition of this inventory we hope to provide policymakers, businesses and users with helpful information and practical guidance to create the necessary environments to reach this common objective. Building upon the vision of former Chair of the EBITT Commission and BASIS initiative[1], Talal Abu-Ghazaleh, when he launched the first edition of this inventory, the second edition continues to provide a brief description of the issues, where they are being addressed and a synopsis of the ICC positions and recommendations. For more detail, the reader can consult the full length policy statements and practice toolkits on a given topic. This inventory will help governments, businesses and consumers to do their part in making the most of ICTs, the Internet and the Information Society. We would like to recognize the leadership of Talal Abu-Ghazaleh in starting this inventory and the efforts of Thomas Pletscher, Secretary General, ICC Switzerland, who led the project for the 1st edition

Herbert Heitmann
Chair, ICC Commission on E-Business, IT and Telecoms (EBITT)

[1] BASIS initiative (Business Action to Support Information Society): BASIS serves as the voice of businesses from around the world on Internet governance and information and communications technologies (ICTs) issues. These tools are key drivers of the global economy, essential for the development of companies and countries.

Introduction

How to use this inventory

The brief synopses of each issue in this inventory are meant to inform and assist decision-makers, businesses and users worldwide in formulating government policy relating to the use and development of ICTs. We encourage you to use these positions, recommendations and information in your country, and to disseminate them widely, while attributing them to ICC. If you would like more information, please contact the ICC International Secretariat at ebitt@iccwbo.org.

This inventory is structured in 6 sections:

SECTION I. Internet and Telecoms Infrastructure and Services
SECTION II. Protection of Personal Data and Privacy
SECTION III. Technical and Continued Development Aspects of the Internet
SECTION IV. Security and Authentication
SECTION V. Legal Aspects
SECTION VI. ICT: regulatory and market issues
ANNEX

Further information and other ICC work products on a range of issues are available on the ICC website: www.iccwbo.org/policy/ebitt/

EBITT commission fact sheet 2010
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/EBITT%20Final%20Factsheet%2011.04.07.pdf

If you need more information about any of the information in this inventory, or on other relevant ICT, Internet and e-business related issues, please contact the following members of ICC International Secretariat at its headquarters in Paris:

Ayesha Hassan, Senior Policy Manager, Executive in charge of ICT Policy
Elizabeth Thomas-Raynaud, Policy Manager
Anna Katharina Moellers, Assistant, EBITT and BASIS

We hope that this inventory will be useful to readers from around the world.

Table of Contents

Foreword ..... **i**

Introduction ..... **ii**

ICC Commission on E-Business IT and Telecoms

EBITT leadership and task forces 1

EBITT policy statements and practice tools 3

SECTION I: Internet and telecoms infrastructure and services **6**

A. Multilateral trade negotiations: telecommunications and e-business 6

B. Telecommunications liberalization 8

C. Government IT procurement 10

D. Global IT sourcing 13

E. Broadband deployment 14

F. Voice over Internet Protocol (VoIP) 16

G. Delivery of audio-visual content over the Internet 17

H. Internet content regulation 19

I. Storage of traffic data for law enforcement purposes 21

J. Digital convergence 23

K. Global Business Recommendations and Best Practices for Lawful Intercept Requirements 25

SECTION II: Protection of personal data and privacy **26**

A. Privacy protection regimes 26

B. 'Spam' 28

SECTION III: Technical and continued development of the Internet **29**

A. Internet Protocol version 6 (IPv6) 29

B. Internationalized Domain Names (IDNs) 31

SECTION IV: Security and authentication **32**

A. Cybercrime 32

B. Electronic authentication 34

C. Information compliance 36

SECTION V: Legal aspects 39
A. Jurisdiction and applicable law 39
B. Electronic Contracting 41

SECTION VI: ICT: regulatory and market issues 42
A. Open source software 42
B. Mandatory certification requirements 44

ANNEX 46
I. What is Business Action to Support the Information Society (BASIS)? 46
II. Overview of Forums 47

ICC Commission on E-Business IT and Telecoms (EBITT) Leadership and Task Forces

Chair – Herbert Heitmann, Executive Vice President, External Communications, Royal Dutch Shell

Vice Chairs
Joseph H. Alhadeff (Oracle, USA)
Stefan Bernhard (Bird & Bird, Sweden)
Gerard Hartsink (ABN AMRO, The Netherlands)
Christopher Kuner (Hunton & Williams, Belgium)

Advisor to the Chair – Kim Ambler (Helix Policy Group, USA)

EBITT Task Forces

Task Force on Internet & Telecoms Infrastructure and Services
Co-Chair – Eric Loeb (AT&T, USA)
Co-Chair – David Appasamy (Madura Micro Finance Limited, India)

Task Force on Privacy and the Protection of Personal Data
Chair – Christopher Kuner (Hunton & Williams, Belgium)

Task Force on Security and Authentication
Co-Chair – Jacques Beglinger (Beglinger Legal Office, Switzerland)
Co-Chair – Christiaan van der Valk (TrustWeaver, Sweden)

EBITT Commission and Task Forces and how they work

Business leaders and experts drawn from the ICC membership establish the key business positions, policies and practices on e-business, information technologies and telecommunications through the EBITT Commission. With members who are users and providers of communications networks and services, information technology and electronic services from both developed and developing countries, ICC provides the ideal platform to develop global voluntary rules and best practices for these areas. Dedicated to the expansion of cross-border trade, ICC champions telecom liberalization and development of infrastructures that support global online trade and the integration of information and communication technologies (ICTs) for economic growth and social development.

Objectives

- Promote the development of electronic business and the integration of information and communication technologies through policies, standards of practice and guidelines that encourage competition, growth and the secure and free flow of information
- Formulate policies on critical telecommunications, information network security, data protection and privacy, trade-related matters, technical coordination of the Internet, and jurisdiction and applicable law in e-commerce issues based on a consensus-building process
- Provide an industry interface on telecommunications, information technology (IT) and e-business issues, with relevant intergovernmental organizations, including: World Trade Organization (WTO), World Bank, United Nations Conference on International Trade Law (UNCITRAL), Organization for Economic Cooperation and Development (OECD), G-8, G-20, UN/CEFACT, UN-Internet Governance Forum (IGF), International Telecommunication Union (ITU), and the European Parliament and Commission of the European Union (EU)

Membership

Commission members include a cross-section of senior corporate and policy executives, and lawyers representing users and providers of goods and services online and offline; telecommunications service providers; online content providers; IT equipment manufacturers and competitive service providers from a multi-sectoral group of companies. Members represent over 35 countries, and include both large multinationals and small and medium size enterprises based in developed and developing countries.

Priorities

Vital questions for e-business and information technology development include telecom liberalization, liability exposure, data protection and privacy, technical coordination of the Internet, consumer confidence in e-transactions, cybercrime, information and network security, and jurisdiction and applicable law in e-commerce.

EBITT policy statements and practice tools

Policy statements

SECTION I: Internet and telecoms infrastructure and services

Global Business Recommendations and Best Practices for Lawful Intercept Requirements
June 2010
http://iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373492LawfulInterceptPolicyStatementJune2010final.pdf

Digital convergence: an economic opportunity
http://www.iccwbo.org/uploadedFiles/Digital_convergence.pdf

ICC Statement on Regulating the Delivery of Audiovisual Content over the Internet
July 2007
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/ICC_policy_statement_on_regulating_the_delivery_AV_content_over_the_Internet__Approved.pdf

ICC policy statement on WTO telecom services negotiations
June 2005
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373-463_WTO.pdf

ICC policy recommendations on global IT sourcing
December 2005
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373-461rev_Global_IT_sourcing.pdf

Common Industry statement on storage of traffic data for Law Enforcement Purposes
June 2003
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/Common_Industry_Statement_on_Storage_of_Traffic_Data_June03.pdf

ICC's strategic objectives for multilateral trade negotiations to ensure a trade regime that facilitates competition in telecommunications and e-business
July 2002
http://www.iccwbo.org/id504/index.html

Storage of traffic data for law enforcement purposes
November 2002
http://www.iccwbo.org/home/statements_rules/statements/2002/373-22-106E.pdf

Broadband deployment
November 2002
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373-21-110E.pdf

The Impact of Internet content regulation
November 2002
http://www.iccwbo.org/id510/index.html

SECTION II: Protection of personal data and privacy

ICC policy statement on 'spam' and unsolicited commercial electronic messages
December 2004
http://www.iccwbo.org/home/e_business/policy/373-22_114_spam.pdf

Employee privacy, data protection and human resources
December 2003
http://iccwbo.org/id543/index.html

SECTION III: Technical and continued development aspects of the Internet

Issues paper on Internationalized Domain Names
July 2007
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/Issues_Paper_on_Internationalized_Domain_Names.pdf

Deploying the next generation Internet: ICC statement on the introduction of IPv6
June 2004
http://www.iccwbo.org/home/e_business/policy/373-%2031_%207_%20IPv6.pdf

SECTION V: Legal aspects

ICC framework for consultation and drafting of Information Compliance obligations
June 2006
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373-472_information_compliance.pdf

ICC recommendations to signatory states to contemplate when implementing the Council of Europe Cybercrime Convention and its First Additional Protocol
March 2003
http://www.iccwbo.org/home/statements_rules/statements/2003/4%20ICC%20key%20recomendations%20to%20signatory%20states.pdf

SECTION VI: ICT: regulatory and market issues

Mandatory certification requirements for IT products and services
March 2009
http://iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/ICC%20statement%20mand%20certif.pdf

Open Source Software
December 2005
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373-466_open_source_software.pdf

Practice tools

SECTION I: Internet and telecoms infrastructure and services

Telecoms Liberalization, An international business guide for policymakers, Second Edition
October 2007
http://www.iccwbo.org/policy/ebitt/id2298/index.html

Procuring ICTs, An Industry Analysis of best practices for government decision-markers
December 2004
http://www.iccwbo.org/policy/ebitt/id2288/index.html

SECTION II: Protection of personal data and privacy

European Commission revision of Standard Contractual Clauses (SCC) the Transfer of Personal Data from the EU to Third Countries (controller to processor) following ICC negotiation
February 2010
http://www.iccwbo.org/policy/ebitt/index.html?id=34969

Standard Application for Approval of Binding Corporate Rules for
the Transfer of Personal Data outside the EU
July 2006
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/Standard_Application_for_Approval_of_BCRs.pdf

Final Approved Version of Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries (controller to controller transfers)
January 2005
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/ICC%20model%20clauses+FAQs%20final%20approved%20%20Jan%202005.pdf

Privacy toolkit, An international business guide for policymakers
August 2004
http://www.iccwbo.org/policy/ebitt/id5289/index.html

SECTION III: Technical and continued development aspects of the Internet

Securing your business, A Companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems. Towards a culture of security
July 2004
http://www.iccwbo.org/policy/ebitt/id2291/index.html

Information security assurance for executives
December 2003
http://www.iccwbo.org/policy/ebitt/id2132/index.html

SECTION I: Internet and telecoms infrastructure and services

A. Multilateral trade negotiations: telecommunications and e-business

Issue

Multilateral trade negotiations can impact competition in telecommunications and the growth of e-business.

Forums where this issue is discussed and/or addressed

Asia-Pacific Economic Cooperation (APEC)
Organization for Economic Cooperation and Development (OECD)
World Trade Organization (WTO)
National Trade Commissions

ICC concerns, recommendations, positions

World business has five core objectives for multilateral trade negotiations:

- Development of the domestic and global infrastructure necessary to conduct e-business while avoiding barriers that would hinder such development
- Full implementation of existing commitments and further liberalization of all basic telecommunications, value-added and computer and related services
- Development of trade in goods and services via e-business
- Strong protection of intellectual property made available over digital networks
- Elimination of Foreign Direct Investment ownership restrictions (FDI)

1. To promote the development of the domestic and global infrastructure, necessary for e-business, world business seeks:

   - The elimination of duties on all IT products in line with the goals of full realization of the objectives of the Information Technology Agreement (ITA), including commitments at the broadest possible level for categories 84, 85, and 90. Refer to: http://www.wto.org/english/tratop_e/inftec_e/itadec_e.htm
   - Full market access and national treatment commitments for the sectors that are associated with the infrastructure and services needed for business-to-business (B2B) and business-to-consumer (B2C) e-commerce
   - An open competitive market for electronic commerce, including commitments not to impose new barriers to the development of the e-commerce infrastructure and services

2. To promote full implementation of existing commitments and further liberalization of all basic telecommunications, value-added and computer and related services, ICC seeks:

   - Market access and national treatment commitments for all service sectors without restrictions; Earlier implementation dates; Reductions or elimination of foreign ownership restrictions; Adherence to the "Reference Paper" commitments for basic telecommunications services only; Compliance with the GATS Annex on Telecommunications for access to and use of public telecommunications networks for the provision of value-added services, including Internet services, and other sectors for which countries have made commitments

3. To promote the development of trade in goods and services via e-business, ICC seeks:

   - Recognition that current commitments under the General Agreement on Tariffs and Trade (GATT), the General Agreement on Trade in Services (GATS) and the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) apply to e-commerce

   - Trade treatment and classification of an electronic transmission that is no less favorable than the historical treatment applied to the underlying good, service, or intellectual property

   - Scheduling of commitments at the highest level possible, including, the adoption of an approach in which parties make full market access and national treatment commitments such that all sub-sectors are covered for relevant service sectors

   - An agreement that existing international classification schemes, such as those used in GATS schedules, should be flexible enough to accommodate technological progress in the online delivery of services

   - An agreement that valuation of digitizable products delivered on a physical medium, including software pursuant to GATT decision 4.1 on Valuation of Carrier Media Bearing Software for Data Processing Equipment, for customs purposes, be based on the value of the physical medium only

   - Make permanent the moratorium on imposing customs duties or other border measures on electronic transmissions

4. To promote strong protection of intellectual property made available over digital networks, ICC seeks:

   - Effective and timely implementation and enforcement of the WTO Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS)

   - Timely ratification of the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty which ensures balance between the rights and obligations of network operators, service providers, and content providers, and users.

B. Telecommunications Liberalization

Issue

Telecoms liberalization means introducing competition into the telecommunications sector by allowing commercial enterprises to set up new telecoms businesses as long as they comply with certain government defined policies, rules and regulations.

Liberalization in this market sector drives the following goals:

1. New investment
2. Upgrading national infrastructure
3. Creating jobs
4. Contributes to improving universal access
5. Improves services, prices, choice for end users
6. Encourages innovation
7. Free flow of information

ICC recognizes these benefits and thereby supports the liberalization of the telecommunications industry.

Forums where this issue is discussed and/or addressed

International Telecommunications Union (ITU)
Internet Governance Forum (IGF)
Global Alliance for ICT and Development (GAID)
Organization for Economic Cooperation and Development (OECD)
World Trade Organization (WTO)
Asia Pacific Economic Cooperation (APEC)
National Regulatory Authorities

ICC concerns, recommendations, positions

The potential benefits of a liberalized telecommunications market are well documented. Telecoms Liberalization has brought more, better and innovative communications services, job growth, new ways to communicate a boost to overall economic growth and the runaway success of the Internet. There are still, however, many countries that have yet to enjoy these benefits. Countries that begin or re-start a stalled liberalization should consider the following principles and challenges in achieving the goals:

- Require getting support 'from the top'. ICC believes that a successful liberalization is most likely to be achieved if support at the highest political and administrative level is available.
- Laws and regulations must be clearly defined and transparent. The government and legislature should seek comments and feedback on proposals leading to liberalizations. Having received these comments, legal and regulatory policies and procedures that are adopted should have certainty. Only by so doing will the liberalized markets attract investments.

- The liberalizing country should draw up a clear 'timeline' for the liberalization initiative. This is especially important if the country elects to liberalize in 'phases'.
- To open up monopolistic telecommunications markets, an effective and independent regulator should be established. The regulator should implement laws and regulations adopted by the government and act as a 'referee' between market players. To be able to do this effectively, independence is necessary.
- Countries that have joined, or plan to join, the WTO should ensure that they have signed up to, and implemented, the reference paper concerning essential competitive safeguards for telecoms liberalization.
- Licensing requirements should not stifle market entry, and barriers to entry must be low. ICC therefore recommends that 'general' telecommunications licenses should be awarded in adherence with objective and non discriminatory principles; licenses should be transparent. Only licenses concerning scarce resources should be limited; and the number of 'general licenses' should be unlimited.
- Whilst keeping a close watch to ensure that anti-competitive behavior does not develop in the national telecommunications market, national markets should be allowed to develop with minimum regulatory hindrance, and should minimize regulatory hindrance on development of the Internet. National regulators should not automatically impose 'legacy regulation' on new technologies like the Internet and new fiber-based broadband networks. Furthermore, once competition evolves in the formerly monopolistic markets, sector specific regulation should be reduced to a minimum.
- ICC believes that technology and innovation is the best enabler of improving universal access of telecommunications services. To maximize the positive contribution of new entrants in delivering universal access, national governments should not provide special 'universal access funding unless it can be provided to all in a 'competitively neutral' manner.

A liberalized telecommunications market brings clear benefits to countries: both directly and indirectly. Whilst the challenges and the specific instruments in achieving an effectively liberalized market differs from country to country, ICC considers its' Telecoms Liberalization Guide to provide countries that begin liberalization with considerations, perspectives and goals that have a universal validity, reflecting the experience of ICC telecoms experts over two decades.

C. Government IT Procurement

Issue

Greater use of information and communication technologies (ICTs) by governments provides benefits that are exponentially related to costs, particularly in developing economies. The benefits of increased use by governments of ICTs are significant and felt throughout the entire economy. ICC promotes the development of a procurement system that maximizes the best value for government investments in ICT, which is compatible with the WTO Government Procurement Agreement.

Governments are one of the world's largest purchasers of goods and services and often the largest buyer of ICT services in their home countries.

Governments have a domestic responsibility to act in a manner that maximizes the benefit of ICT services to them and the citizens, and to purchase those ICT services in a manner that fosters competition domestically.

ICC produced a best practice document entitled, "Procuring ICTs", which identifies how effective governmental ICT purchases should be conducted in order to maximize benefits and further real domestic competition in the supply of ICT services.

Forums where this issue is discussed and/or addressed

European Commission
World Trade Organization (WTO)
National Governments

ICC concerns, positions, recommendations

Government procurement policies can often be slow, which sometimes reduces the economic benefit of ICT solutions to government. The following benefits of ICTs have been identified:

- Government ministries benefit from increased productivity.
- Citizens benefit from increased access to information.
- ICT companies benefit from increased opportunities (to sell services) and to gain experience in new systems.
- The national economy benefits from ICTs by having private ICT solutions interacting with governmental ICT solutions.

To maximize these overall benefits it is important that national governments use a procurement system which includes the following set of characteristics:

- Efficiency – good value for money in public expenditure
- Flexibility – adapts to changes in a country's public administration needs
- Compatibility – meets international obligations (WTO and EU rules)
- Openness – unrestricted and universal access to the procurement market
- Transparency – selection of bidders, tendering process, and the award of contracts is open to public examination
- Integrity – addresses problems of fraud and corruption through mechanisms for prevention and detection

ICC recommends the following issues be considered to achieve the above:

1. Policy aspects of ICT procurement

Governments should recognize that they are a very substantial national purchaser of ICT and should act in a manner which fosters competition; this can be done by acting in a compliant manner and/or splitting contracts thus creating multiple contracts. Governments should additionally ensure that bidding processes are clear and simple and should adopt anti-corruption measures.

2. Industry bid decision process

Governments should run a procurement process to attract and maximize competition and to create positive relationships with its contractors. To achieve this, governments should realize that potential suppliers assess a bid from the following main criteria:

- Is the procurement real?
- Can the business do it?
- Can the business win it? and,
- Does it make good business sense?

Each of these criteria raises numerous additional questions, information requirements and procurement policy questions. Governments must appreciate this and act in a manner which allows potential suppliers to assess each criteria in a meaningful manner.

3. The procurement process

A procurement process, depending upon size and complexity, should often consist of the following:

- Needs definition / requirements
- Request for Information
- Request for Comments
- Request for Proposal
- Proposal
- Live test and demonstration
- Best and Final Offer
- Award
- Appeal procedures

Governments are very substantial buyers of ICT and also potential beneficiaries of ICT services if they procure the right service at the right price. To achieve all benefits of ICT, it is crucial governments apply an efficient and transparent procurement process where the right supplier is chosen after a tendering process in a competitive market. Given the size and, frequently, complexity of the ICT procurement, a number of separate steps need to be considered and taken by the government and its potential suppliers.

D. Global IT Sourcing

Issue

Modern business models around the world are increasingly organized across national boundaries. Global sourcing allows companies to geographically distribute different corporate activities around the world. This refers to a process by which manufacturing or service needs are procured from an outside source; which can be independent or within the same business groups that does the sourcing.

Forums where this issue is addressed and/or discussed

Organization for Economic Cooperation and Development (OECD)
National governments
World Trade Organization (WTO)

ICC concerns, positions, recommendations

A significant portion of the economic activity of companies is a consequence of local market growth. The investment required in large, double-digit-growth markets is significant and should not be underestimated.

Virtually all global firms have established significant IT enabled services (ITES) centers in India and other emerging markets, including China, Russia and the Philippines. Most experts seem to agree that global sourcing will grow. Major global companies in most industry sectors are moving to global sourcing policies, seeking best-value services from any location. This is not just a cost savings measure but also a response to increase efficiency, stay competitive and respond to new emerging demand in an increasingly global market.

One aspect of global sourcing that is just beginning to be explored is its potentially positive impact on a country's economy as a whole. With time, as economies evolve, both activities and locations evolve as well. Locations can improve their business environment by investing in skills, open markets, infrastructure and innovation. Locations can also worsen by increasing taxes, adopting restrictive social policies, corruption and political instability. These combined changes affect companies' global sourcing strategies on a continuous basis.

In opposing measures adopted by governments to restrict global sourcing, ICC instead recommends that:

- Companies need to be able to maintain flexibility to source globally to meet the needs of their own particular business model.
- Governments embrace global sourcing as a means to improve economies by taking constructive actions to encourage innovation, create an enabling business environment, and create an educated and skill-based workforce.

E. Broadband Deployment

Issue

Broadband is one of the key innovative technologies and services in the market today. Increased access speeds and geographical coverage require certain conditions to be in place.

Forums where this issue is discussed and/or addressed

European Union Institutions
Internet Governance Forum (IGF)
International Telecommunication Union (ITU)
Organization for Economic Cooperation and Development (OECD)
Asia Pacific Economic Cooperation (APEC)
National Governments

ICC concerns, recommendations and positions

Liberalization and competition in the telecommunications market have brought new and innovative technologies and services to the market. A market-driven broadband policy that ensures the right market conditions for infrastructure investment and innovation is essential to the ongoing deployment of broadband. This market-driven framework must be technology-neutral and market-led. Otherwise, the potential for broadband deployment may be easily stifled.

What are the optimal framework conditions?

Creating an optimal framework requires a mix of policies to stimulate conditions for the supply of the infrastructure, demand for the infrastructure, and certain specific public policy concerns. The ability of broadband providers to maintain and invest in a robust and expanding broadband infrastructure requires a coordinated and unified policy approach from government departments and agencies that supports private sector investment and innovation. The public sector has a key role to play in establishing the right regulatory and political framework, and also by adopting and using broadband itself as a demand-side driver for investment. ICC proposes the following actions by government to promote a business climate conducive to investment in broadband infrastructure and services and products that require higher bandwidth and enhanced service quality.

Supply of Broadband Infrastructure

1. Ensuring a competitive marketplace:

Governments should ensure a pro-competitive and market-driven policy framework that promotes investment in and deployment of broadband for business users as well as consumers. This framework should include the following:

2. Ensuring efficient and effective frequency allocation and management procedures:

Governments should make available the maximum radio spectrum available for the deployment of advanced broadband services and thus ending the current artificial scarcity of spectrum.

3. Promoting access in rural, remote and under-served areas:

In some cases, governments can promote access to broadband infrastructure in rural, remote or under served areas. However, in so doing, governments should consider the cost / benefits to be derived from such policies. Any policy implemented must be transparent and neutral with regards to effect on competition, investment and innovation.

Demand for Broadband Infrastructure

- WTO / trade liberalization of products and services delivered via broadband.
- Governments should assist market demand by becoming an early adopter of broadband; for example via e-government.
- Government could also assist market demand by focusing on small to medium enterprises (SMEs); for example via e-procurement.
- Regional and local governments could be used to consolidate demand where demand may not have developed otherwise. These policies should not be allowed to distort the market or create barriers to entry.
- Governments can assist market demand by stimulating IT education and training.

Public Policy Issues Related to Broadband Use

ICC considers that the following aspects must be considered by governments in formulating public policy relating to broadband:

- Governments should promote a culture of security in the broadband sector;
- Governments should ensure that appropriate legislation is in place to investigate and combat cyber crime; and
- Effective enforcement of intellectual property
- Public policies should promote, not deter, investment in next generation broadband technologies that can enable new bandwidth-intensive and quality-sensitive applications and services.

F. Voice over Internet Protocol (VoIP)

Issue

Internet Protocol (IP) enabled services, including Voice over Internet Protocol (VoIP), represent an important shift in telecommunications technology. This shift to IP networks enables innovative converged voice, data and video applications. Business and consumer users are examining how to take advantage of the efficiencies and advanced communications capabilities of IP-based technology.

Forums where this issue is discussed and/or addressed

Internet Protocol version 6 (IPv6) forum
Organization for Economic Cooperation and Development (OECD)
National Regulators

ICC concerns, recommendations and positions

ICC believes that VoIP has the potential to bring benefits to business users and consumers in both developed and developing countries by increasing competition and expanding ICT offerings. To ensure that VoIP can reach its full potential and is not stifled by unnecessary or poorly tailored regulation, ICC recommends that governments consider the following aspects:

- Policy makers will maximize the competitive and user benefits of VoIP by creating a policy framework that encourages the continued development of an IP-enabled service environment.

- Regulatory agencies should adopt a 'light touch' approach that focuses on encouraging competition and maximizes flexibility for the introduction of VoIP services, while respecting the need to ensure consumer protection.

- An essential first step is for all governments to ensure that VoIP services are open to provision by all interested service providers, including incumbents and new entrants alike, and that where licensing conditions exist, they are objective and non-discriminatory, and the criteria for granting authorizations are transparent.

- VoIP offers real differences in services, which will result in consumer benefits as well as some consumer challenges. These differences merit a flexible regulatory approach that is not tied reflexively to traditional regulation. Work with business to ensure that public interest considerations including numbering, emergency services, universal service and cooperation with law enforcement are addressed adequately and do not distort competition between PSTN and VoIP services.

- Recognize the distinct potential of VoIP technology and allow all interested service providers to provide IP-enabled services;

- Recognize the manner in which VoIP can better enable enterprise customers to expand their cost-effective operations to a country by utilizing VoIP (e.g. economic growth through ICT-enabled services such as VoIP); and

- Adopt a light handed approach with reliance on general competition law wherever possible and limited application of ex ante regulation as set forth above.

G. Delivery of Audio-Visual Content over the Internet

Issue

Due to the present growth of 'streaming' audiovisual content over the Internet and mobile wireless devices, some countries (such as European Union member states) are now considering the establishment of regulatory regimes governing this 'streaming' of audiovisual content.

Forums where this issue is discussed and/or addressed

European Union Institutions
Organization for Economic Cooperation and Development (OECD)

ICC concerns, recommendations, positions

- Self regulation is the preferred option for ICC members
- The 'country of origin' principle for applicable jurisdiction should prevail to ensure regulatory certainty

The ICC policy statement focuses on the extension of regulations to cover audiovisual content over the Internet but the ICC business community believes that the traditional broadcasting regulation as a whole should be reviewed in order to determine its relevance vis-à-vis its underlying goals in an ever changing technological environment.

The Internet is a global phenomenon which consists of a vast number of interconnected, national and/or multinational, networks. These intelligent networks connect hundreds of millions of end users and involve millions of businesses in its operation. ICC does not believe that the application of stringent regulatory controls on this global and evolving infrastructure is well suited as it runs the risk of stifling creativity and skewing investment. Self- and co-regulatory mechanisms have effected an entire submarket of 'controls', used widely by end customers, which include content rating, parental controls, and filters that empower parents to self control the type of content received.

In this market sector, ICC instead recommends self regulation, which will particularly:

- Keep barriers to entry low;
- Foster innovation; and
- Enhance competitiveness.

Specifically, ICC believes that only self regulatory tools can embrace the dynamic and evolving nature of the Internet. Self-regulatory tools respond rapidly to market and consumer concerns and result in lower costs for the industry and tax payers. Additionally, ICC views the fact that the Internet with its hundreds of millions of users and millions of content providers cannot and should not realistically be 'regulated' in the traditional sense by traditional national regulators.

The global nature of the Internet does not lend itself to effective national regulatory intervention; and further, such regulation could curtail the development of Internet services and related innovation.

In fact, ICC considers the open, innovative and global nature of the Internet an aspect that should be promoted and not tampered with. The Internet should remain an open, global, network with low barriers to entry.

Self-regulation does not mean 'no-regulation'. Many complementary rules and regulations of general application will continue to apply on audiovisual media transmitted over the Internet, just as it applies for other media. These rules and regulations relate, for example, to the protection of minors and human dignity.

The potential extraterritorial impact of Internet content regulation must be considered. The decentralized and global nature of the Internet does not lend itself to national attempts to regulate any content distributed over the Internet. To overcome this problem, ICC supports that the delivery of audiovisual content over the Internet should be governed by the 'country of origin' principle. Specifically, there should be a mutual recognition and respect between national regulators approaches to self regulation.

Moreover, the 'country of origin' approach is the only realistic approach in terms of arriving at reasonably cost effective regulatory measures in this global market segment; any other approach would necessitate that broadcasters and content providers ensure compliance with every country's national self-regulatory approach. ICC believes that the costs of this approach would be excessive and drive content providers from the global market.

Self-regulation is most likely to be in the consumers' interests, as it most often affected at the edge of the Internet, using a choice of customer-empowered technologies and filters, where 'content regulation' is most likely to be effective. Moreover, self-regulation is the most easily updated and flexible, and thus most likely to keep apace with the global and dynamic reality of the internet. Some current examples of this approach include: Classification of Audiovisual Media, Internet Watch Foundation, Childnet and GetNetWise.

The 'streaming' of content over the Internet is globally increasing; both with regards to download and upload. The Internet and the users of the Internet are global in nature and the delivery of audiovisual content over the Internet must be treated as such. ICC therefore recommends a strong reliance upon 'self regulation' and adherence to the 'country of origin' principle for the purposes of establishing jurisdiction.

H. Internet content regulation

Issue

Internet content regulation refers to any type of legislation by governments or regulatory authorities directed at: 1) censoring information and communication on the Internet based on subject matter; and, 2) controlling, or attempting to control, access to Internet sites based on subject matter.

Forums where this issue is discussed and/or addressed

Council of Europe
Internet Governance Forum (IGF)

ICC concerns, recommendations and positions

The Internet continues to be a growing, vibrant and important medium for conducting business. Indeed, the Internet and e-commerce facilitate international trade. Given the benefits of increased trade for society, governments should refrain from imposing unnecessary restrictions on Internet content.

It is important to note that ICC recognizes legitimate public policy objectives such as protecting the general public, and particularly children, from objectionable Internet content and prohibiting use of the Internet for criminal activity and information that could be prejudicial to global security. We believe that such regulations should be kept to a minimum so as not to restrict the free flow of information, and to respect for human rights.

ICC proposes the following principles and strategies be considered by legislatures, regulatory bodies, and courts in making determinations regarding regulation of content on the Internet.

ICC encourages governments and legislators to cooperate with business to address these important issues.

- Allow self-regulation to demonstrate its efficacy – customer filtering tools, labeling and other self-regulation efforts on the Internet should be preferred over legislative mandates;
- When necessary, regulation should be kept to a minimum and only deal with specific, observed abuses, taking account of existing technologies; and
- When necessary, laws and regulations should be clear, precise and narrowly tailored.

When regulation is required, attention should be paid to the following considerations:

a) The domestic and international consequences of the proposed regulation in terms of cost and impact on the development of the Internet and e-commerce;

b) The underlying technical issues and the precise responsibilities of each of the relevant Internet actors;

c) An assurance that potential criminal actions are described in clear and objective terminology; and

d) Recognition that developing technologies can generate unique observed abuses, relevant regulations should endeavor to be as technology-neutral as possible.

To ensure the quality and clarity of regulation, ICC strongly encourages a transparent and inclusive consultative process, including regular exchange of information between the public and the private sectors.

- Legislation should not place additional costs and burdens on business.
- Jurisdiction and applicable legal mechanisms should not subject business to the risks of unexpectedly being subjected to laws and judgments in other countries.
- Provisions dealing with liability should limit the liability of technical service providers and carefully balance the interests of all stakeholders in the electronic environment.

Lawmakers are encouraged to consider the effects of the points above and engage in critical dialogue with businesses worldwide to ensure the continued growth and vigor of the Internet by providing legal certainties with the least possible burdens and constraints.

I. Storage of traffic data for law enforcement purposes

Issue

Many countries impose obligations on communications service providers ("CSPs") [including Internet service providers] to store end-user traffic data for possible use by law enforcement agencies ("LEAs"). Some countries impose mandatory data retention and/or extended periods of time in which the data must be available.

Forums where this issue is discussed and/or addressed

National and regional governmental bodies

ICC concerns, recommendations, positions

ICC urges governments to co-ordinate toward a data retention regime based on existing storage of end-user traffic data for legitimate business purposes and to seek advice and opinions from key industry stakeholders. Insufficient public input and multi-lateral harmonization is likely to result in policies that harm CSPs and their end-users and impair a competitive and dynamic communications and IT services market.

Traffic data" concerned

Although traffic data generally means the 'log' information which is created every time someone uses a communications system, it does not include the actual 'content' of the communications. Furthermore, the scope of what constitutes a 'log' will often vary by country, provider and service provided.

Broad definitions and wide-reaching laws

Businesses are concerned that national governments may define 'traffic data' so widely as to encompass data related to communication and that such an open ended definition would increase technical and cost burdens on CSPs in addition to damaging public confidence in the privacy of electronic communications.

Whilst businesses are supportive of legitimate and realistic measures to combat terrorism there is concern that some of these goals could be adequately met by narrower, more targeted powers of data retention.

Data preservation versus data retention

Several countries are considering whether to require CSPs to store the communication of a particular individual for a finite period as specified under the appropriate judicial authority (data preservation) or to require the CSP to retain all of certain types of the traffic data created by all users (data retention). ICC members strongly believe that data preservation should be favored because it is less burdensome and costly that data retention and less harmful to public confidence.

Cost to businesses

The costs associated with data storage are immense. Not only do these costs add to the overall costs of the business but the additional privacy and security issues are created by the creation of enormous pools of stored data.

To address these concerns, any traffic data storage requirements introduced must balance the needs of LEAs, the capabilities and interests of CSPs, and the interests and rights of end-users.

J. Digital convergence

Issue

Convergence refers to the evolution of previously distinguishable digitalized information formats, services, applications, networks, and business models in ways that reduce or blend the distinctions. Convergence is driven by the rapid development of digital technology. The convergence phenomenon presents a huge opportunity for all stakeholders to improve economic efficiency and productivity, leading to innovation, new business opportunities, increased choice and lower prices that benefit all users. It can also provide the developing world an unprecedented opportunity to participate in the digital economy. Digitalized information flows have already increased market access and competitiveness by creating greater efficiency and global scope of sales and service.

As markets develop, their structures are affected by changing technology, creating opportunities for new business models, increasing competition, and challenging and altering existing businesses and traditional business models. Changes to the affected industries' economics will also challenge the existing regulatory and legislative norms and cause a wide range of stakeholders to re-consider their relationships with the affected sectors. Convergence refers to the evolution of previously distinguishable digitalized information formats, services, applications, networks, and business models in ways that reduce or blend the distinctions. Convergence is driven by the rapid development of digital technology.

Forums where this issue is discussed and/or addressed

European Union Institutions
Internet Governance Forum (IGF)
International Telecommunication Union (ITU)
Organization for Economic Cooperation and Development (OECD)
National Governments

ICC concerns, recommendations, positions

ICC urges governments to work in partnership with business to enable convergence and ensure that regulation neither creates unnecessary burdens nor unintended consequences that could impair the potential for economic growth and societal benefit that deployment of these technologies and/or new business models can provide. Markets and business models are changing rapidly and inappropriate intervention could hamper these beneficial changes. The unconstrained market has already led to huge developments while interventions have sometimes produced chilling effects in important markets.

Governments should evaluate policy frameworks to ensure that obstacles to the deployment of converged business models, and ICTs generally, are removed. ICC urges governments to work in partnership with business to enable convergence and ensure that regulation neither creates unnecessary burdens nor unintended consequences that could impair the potential for economic growth and societal benefit that deployment of these technologies and/or new business models can provide.

Core principles for policymakers

a) a) Government regulation should be limited to promoting competition, innovation and investment, allocating scarce resources and, where necessary, achieving public interest objectives. Any regulation should only be implemented after proper consultation with all stakeholders to ensure its proportionality.

b) Competition law should be used as much as possible as the predominant means of preventing abuses of market power.

c) Given the borderless nature of the Internet, there is a particular need to avoid divergent approaches between countries or regions, which may result in barriers for convergence, the off-shoring of investments to more favourable regulatory climates or, at worst, the balkanization of the Internet. Adequate and effective intellectual property protection and enforcement are essential components to a policy framework that will continue to advance the creativity convergence is helping to fuel.

Benefits

The convergence phenomenon presents a huge opportunity for all stakeholders to improve economic efficiency and productivity, leading to innovation, new business opportunities, increased choice and lower prices that benefit all users. It can also provide the developing world an unprecedented opportunity to participate in the digital economy. Digitalized information flows have already increased market access and competitiveness by creating greater efficiency and global scope of sales and service.

Convergence offers further benefits to society. For example, convergence enables regional development, increases entrepreneurial activity, enhances educational opportunities (including those in remote areas), and access to healthcare and training. It has facilitated significant online social interaction and creative collaboration, also improving the integration of people with special needs and non-traditional working groups into society.

Convergence can be a stimulus within the information society ecosystem for creativity, improved productivity, continuous technological innovation, economic growth, societal benefit and greater inclusion. Convergence facilitates the use and deployment of information communication technologies (ICTs) across all stakeholders - business, government and individuals. It enables content creation, the availability of information anywhere by a multitude of devices and from a multitude of sources as well as communication, collaboration, coordination and interoperability among people, services and applications through enterprise systems and digital networks.

Convergence over the last ten years has referred mainly to the promise of new functionality in ICTs that was afforded by the ability to bridge networks and computing and communication devices. Today, continued evolution of ICTs, with the Internet as a key enabler, has built upon that foundation of network convergence and is reducing the importance of distance, connecting people and speeding information flows and processes – constituting a crucial development in the evolution of interdependent global enterprises and increasing the potential for greater inclusion and enhanced societal interaction.

K. Global Business Recommendations and Best Practices for Lawful Intercept Requirements

Issue

For many decades, as a condition of holding a telecom license, nearly every country has required telecommunications and Internet service providers (collectively "communications service providers" or "CSPs") to cooperate with investigations by law enforcement agencies ("LEAs"), including with LEA requests for lawful intercept ("LI") of communications[2]. Until recently, such licenses and associated regulation imposed specific requirements to build network capabilities to support LI only on a small number of infrastructure operators and mass market voice service providers. Now, driven by the ongoing migration from traditional public switched telephone network ("PSTN") services to Internet Protocol ("IP")-based services (which pose genuine challenges for traditional LI), many countries are adopting and implementing increasingly detailed and costly requirements on many CSPs to build network capabilities that support LI at the demand of LEAs.

Forums where this issue is discussed and/or addressed

National and regional governmental bodies
European Telecommunications Standards Institute (ETSI)
International Telecommunications Union (ITU)
3rd Generation Partnership Project (3GPP)

ICC concerns, recommendations and positions

Unfortunately, some current approaches to LI capability regulation, involving broad LI mandates on all or most CSPs, threaten the development of an innovative, competitive communications market. These approaches can impose significant costs, technological challenges and regulatory uncertainty on CSPs (including by using existing inadequate LI technical standards), and should be consistent with other legal obligations such as those related to information security, privacy and human rights. These issues impact upon businesses across sectors and geographies, both as users and as service providers. To address these challenges, there are specific practical approaches that can provide LEAs with all or most LI capabilities that they reasonably require, while minimizing unnecessary adverse effects on CSPs and the communications market. As detailed in this paper (with eight specific recommendations), these practical approaches seek to balance the interests of LEAs, CSPs, business users and consumers, and to ensure a level playing field for all CSPs.

ICC's recommendations involve:

- Dialogue between governments and CSPs to define clear and transparent LI requirements that proportionately align obligations and benefits specific to individual CSPs;
- Efficient LI implementation through regulatory consistency, adoption of existing international technical standards, and centralized, multi-country LI solutions;
- Public funding of LI capability costs; and
- LI law and regulation that is clear, transparent and judiciously implemented.

[2] LI means the legally mandated capability to intercept communications in the course of transmission between two or more parties, required to support valid law enforcement investigative purposes, and does not include other measures CSPs are required to implement to address other illegal activity over their networks.

SECTION II: Protection of personal data and privacy

A. Privacy protection regimes

Issue

The Internet provides new opportunities and challenges with respect to privacy. Ensuring balanced data protection and privacy regimes that are flexible enough to keep up with societal needs, new technologies and innovations in business methods, and also ensure useful protection of users' personal data, and support the free flow of information present new challenges.

Forums where this issue is discussed and/or addressed

Asia-Pacific Economic Cooperation (APEC)
Council of Europe
European Commission
Internet Governance Forum (IGF)
Organization for Economic Cooperation and Development (OECD)

ICC concerns, recommendations and positions

Governments should further recognize that the Internet is a medium providing new opportunities and challenges. Heavy-handed privacy laws and regulations can have the unintended consequence of stifling innovation and growth. Data protection and privacy regimes need to be flexible enough to keep up with changing societal needs, new technologies and innovation in business methods.

Existing regulatory systems must, of course, provide consumers with useful protection of their personal data, but at the same time must guarantee the free flow of information needed for the information society to produce the anticipated benefits.

Governments should also recognize that government regulation or 'top down' legislation may not be the most effective way to achieve an acceptable level of privacy protection. It is essential for governments to recognize tools for privacy protection developed by industry, and to work together with industry to develop a privacy framework that both furthers privacy protection and promotes economic growth.

ICC encourages governments to take the following steps to achieve optimum privacy protection:

- Adopt principles to ensure adequate data protection, such as those included in this document, and in doing so not exceed the principles set forth in the 1980 OECD Guidelines, and APEC principles.

- Adopt a flexible and responsive approach to the protection of personal information, including the acceptance of self-regulatory solutions and technological innovations that empower the user, determining where specific laws are needed to protect consumers from harm and enact those laws in the most targeted fashion possible.

- Educate the public about privacy protection and the use of privacy-enhancing technologies.
- Cooperate internationally to ensure a seamless environment for different privacy regimes. In assessing the level of protection provided to personal information in other jurisdictions, the criterion should be the objective level of protection afforded by the system as actually used in practice within that jurisdiction.
- Governments should avoid developing laws, policies and practices that create obstacles to trans-border flows of personal data.
- Endorse model contracts, codes of conduct, seal programmes, and other self-regulatory mechanisms prepared by the private sector in order to promote the free and secure flow of information within and between companies, and across borders.

B. 'Spam'

Issue

Businesses and consumers around the world have come to rely on the speed and convenience of e-mail and other types of electronic communications. In the space of a few short years e-mail has become an essential tool to do business, get information, and keep in touch. There has been much controversy about the problem of "spam" and how it may be curtailed. As different legal rules apply to electronic communications in different jurisdictions, there is no generally accepted definition of the term 'spam.' identify illegitimate or unacceptable electronic communications cause users and service providers many problems, and cost burdens.

Forums where this issue is discussed and/or addressed

Organization for Economic Cooperation and Development (OECD)
Internet Governance Forum (IGF)
European Commission

ICC concerns, recommendations and positions

By 'spam', ICC means harmful, fraudulent, malicious, misleading or illegal communications, generally sent in bulk. This is the definition of 'spam' as used in this paper.

Distinguishing between what ICC and its members all agree should be categorized as 'spam' and legitimate commercial electronic communications brings two clear benefits:

a. It recognizes the legitimate needs and benefits of commercial electronic communications, and

b. It allows governments and others to focus on the real problem of harmful, fraudulent, malicious, misleading or illegal communications.

ICC positions:

1. Responsible and legitimate marketing practices are the basis of self-regulation
2. Legitimate marketing-focused electronic communications are not 'spam'
3. Not all 'spam' messages have a commercial intent.

Business endorses a multi-faceted toolkit approach to fighting spam:

- Education and cooperation: Business and government must work together in public-private partnership to educate users and businesses in the fight against spam.
- Technology: Industry should continue to develop technological solutions to spam, working with governments and consumers to promote awareness of technological approaches.
- Industry's role in fighting spam: Business can best manage legitimate unsolicited commercial e-mail with industry codes of conduct and other self-regulatory tools.
- Government enforcement: Governments should ensure that relevant existing legislation covers harmful, fraudulent, misleading or illegal messages and is effectively enforced.

A coordinated effort in each of these areas is the best way to effectively deal with, while ensuring that businesses and consumers can enjoy the convenience and ease of electronic communications.

SECTION III: Technical and continued development of the Internet

A. Internet Protocol Version 6 (IPv6)

Issue

IPv6 is the acronym for Internet Protocol Version 6. IPv6 is the 'next generation' Internet Protocol designed by the Internet Engineering Task Force (www.ietf.org) to follow the current version Internet Protocol. Internet Protocol (IP) is a set of technical rules that governs how information travels around the Internet. The main benefits of IPv6 are a greater number of IP addresses to support growing Internet connectivity, a more efficiently functioning Internet, and better security.

ICC endorses the deployment by business of IPv6, while recognizing the cost and resource issues this transition creates. Governments also need to act to support and encourage IPv6 adoption, while avoiding government-mandated standards and in accordance with principles of technology neutrality. Understanding the benefits and challenges of the new Internet Protocol, IPv6, and the actions business and governments need to take are essential to ensure a timely and smooth transition.

Forums where this issue is discussed and/or addressed

Internet Corporation for Assigned Names and Numbers (ICANN)
Internet Governance Forum (IGF)
Internet Protocol Version 6 Forum (IPv6)

ICC concerns, recommendations, and positions

In order to continue forward progress in the implementation of IPv6, minimize deployment costs, and enable innovative new applications to be developed, it is essential that business and governments understand the benefits and challenges of IPv6. First priorities should include analysis, testing and planning initiatives to ensure the interoperability of IPv4 and IPv6 during a period of smooth coexistence.

- Business should take advantage of scheduled equipment and software upgrades and develop a timeline, program and procedures to upgrade Internet servers and relevant devices to IPv6, recognizing that the upgrade will require costs and impose burdens. This demonstration of leadership by business will encourage other Internet stakeholders and underline the value IPv6 brings to the Internet.

- Business must recognize that the security and stability of the existing network is an essential requirement in the transition period when IPv4 and IPv6 will coexist.

- Business should continue its efforts to improve government and consumer awareness of the importance and benefits of IPv6, for example, through initiatives such as the IPv6 Forum (www.ipv6forum.org), a consortium of vendors, which organizes information events around the world to increase awareness and promote the adoption of IPv6.

- Business should continue to provide expert input into the technical coordination bodies responsible for developing and overseeing IP and its related protocols, particularly the Internet Engineering Task Force (IETF). This input will help ensure that as new technologies develop, they are compatible with and take advantage of IPv6.

Private sector leadership in the technical coordination of the Internet has been responsible for its continued and successful global development. Governments are encouraged to take action to support IPv6 deployment, recognizing that market forces, not government intervention, should be the main driving force for deploying IPv6.

Imposing government-mandated standards or timelines would be an unhelpful approach since this might inhibit targeted deployment efforts or result in inefficient use of limited resources. Government initiatives supporting industry efforts to overcome implementation challenges and increase awareness and prioritization of IPv6 are likely to be more productive and in accordance with the principle of technological neutrality.

B. Internationalized Domain Names (IDNs)

Issue

The introduction of Internet domain names in non-ASCII (American Standard Code for Information Interchange)[3] characters is the subject of much controversy and debate. Some contend that it is an almost trivial exercise while others argue that it is a tremendously complex task that if done too hastily or without proper planning threatens the integrity and stability of the Internet. The Internet Engineering Task Force (IETF) has produced a number of 'Requests for Comments (RFCs)' on the topic[4].

Forums where this issue is discussed and/or addressed

Internet Corporation for Assigned Names and Numbers (ICANN)
Internet Engineering Task Force (IETF)
Internet Governance Forum (IGF)

ICC concerns, positions, recommendations

Potential areas of interest are:

- Policies regarding mixed IDNs
- Uniform Domain Name Dispute Resolution Policy (UDRP) reform
- Maintenance of a unified domain space
- Means of achieving consolidated language tables and character sets

IDNs are an important next step in ensuring that information through the Internet is accessible to all users around the world. ICANN has announced the introduction of the first IDN country code top-level domain names (ccTLDs)

However, if not carefully and centrally implemented, IDNs could destabilize the Internet and disenfranchise the global user from his right to access correctly, efficiently and securely a singular and interconnected database of the global Internet currently available to the global citizen. There is a concern that internationalized domain names may lead to different resolutions and results in a fragmented Internet.

[3] ASCII (American Standard Code for Information Interchange). The ASCII Characters are Latin or Roman language characters with a maximum of 128 defined alpha, numeric and special characters.

[4](See http://www.rfc-editor.org/rfc/rfc3490.txt) that provides guidance on the issue.

SECTION IV: Security and authentication

A. Cybercrime

Issue

Cybercrime involves the use of computers or networks as tools, targets, or places of criminal activity. As technology evolves, the level of sophistication, and damages incurred, of many cybercrime increases. Often the actual crimes are not new, but the means by which they are committed require that governments review their criminal legislation to ensure that the appropriate legislation and resources are in place regardless of the technology used. The borderless nature of the Internet demands a high level of international cooperation in investigating and prosecuting cybercrime.

Business is investing significant resources to assist law enforcement in reducing cybercrime, because it is in the interest of business as well as the consumer to make cyberspace a safe place to shop.

Increased consumer empowerment based on easy recognition of brands and trustmarks and the increased availability and use of filtering and rating technologies - coupled with international cooperation within law enforcement and effective cooperation with the private sector - offer practical means of protecting consumers against fraud and crime on the Internet.

Forums where this issue is discussed and/or addressed

Asia-Pacific Economic Cooperation (APEC)
Council of Europe
Internet Governance Forum (IGF)
International Telecommunication Union (ITU)
Organization for Economic Cooperation and Development (OECD)

ICC concerns, recommendations, and positions

- Businesses constantly develop and deploy measures designed to ensure the security of networks and the content residing on these networks to protect them from attack. However, government action may also be needed to ensure that the necessary laws are in place to make such attacks illegal.

- Governments should ensure similar criminalization of specific cybercrimes and crimes committed in cyberspace to avoid the creation of "cybercrime havens".

- Different nationalities have different legal systems and criminal laws. What might be illegal in one jurisdiction is not always illegal in another. Therefore, arrangements and cooperation mechanisms between enforcement agencies is the appropriate way to deal with cybercrime that crosses borders.

- Governments should refrain from imposing conflicting privacy and security obligations while accommodating and not impeding effective criminal investigation and prosecution.
- When establishing substantive offenses, governments should take care not to inadvertently prevent legitimate and legal activities and further innovation; and
- Security testing should be permitted in a manner that is consistent with existing applicable law.

Cybercrime legislation should:

- Limit service provider liability in a manner that balances the interest of all interested parties including copyright owners, service providers and users
- Provide for reimbursement for costs of compliance;
- Identify the appropriate circumstances for corporate liability;
- Provide for the criminalization of copyright infringements; and
- Adopt clear procedural safeguards for the interception, preservation, production and seizure of data, which would ensure the efficient and expeditious response to law enforcement requests, including a safe harbor for cooperation with law enforcement.

B. Electronic authentication

Issue

Electronic signatures* are important to ensure proper identification of communicating partners, and authenticity and non-repudiation of messages that they exchange Electronic authentication is an embryonic sector that requires a flexible framework of rules to evolve. Self-regulation should be given preference to avoid the lock-in effect of inflexible and potentially incompatible government regulation. Governments have an important role to play in assuring the legal validity of electronic signatures.

Forums where this issue is discussed and/or addressed

Internet Governance Forum (IGF)
National and regional governmental bodies
Organization for Economic Cooperation and Development (OECD)

ICC concerns, authorization positions

- Common definitions and best practice guidelines for authentication and in particular certification practice have been published by several business organizations and will be continually revised to reflect business practice.

- Governments should implement the principles on authentication in the OECD Ottawa Ministerial Declaration.

- The private sector should ensure technical interoperability. The legal acceptability of certificates and electronic signatures, both within a nation and internationally, should be supported by appropriate government policies.

- Government policies should aim to provide a predictable legal framework based on the fundamental concept of freedom of contract. They should be non-discriminatory; technologically and architecturally neutral; promote flexibility as to the content, form and function of certificates and similar authenticating devices – including trustworthy registers of uniquely identified business entities, specified formats and specific-use e-mail addresses; and promote competition among providers of authentication services.

* The terms “digital signature” and “electronic signature” are often used interchangeably. This has led to significant international confusion as to the use of the term. This topic is not appropriate for an in-depth discussion in this paper. We refer interested parties to http://www.iccwbo.org/home/guidec/guidec.asp or www.ilpf.org/work/ca/draft.htm and related information sources for further information and definitions. For the purpose of clarity, the term “digital signature” as used in this document refers to “a transformation of a message using an asymmetric cryptosystem such that a person having the ensured message and the ensurer’s public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key, and (b) whether the signed message has been altered since the transformation was made.” The term “electronic signature” as used in this document refers to “a signature in electronic form in, or attached to, or logically associated with, a data message, and used by or on behalf of a person with the intent to identify that person and to indicate that person’s approval of the contents of the data message.”

- Rules for evaluating the legal validity of electronic signatures should not be written to require localization, local partners, local insurance or guarantee schemes, mutual recognition, or otherwise act as trade barriers.

- Standards for electronic signatures that are used or recognized by governments should be technology neutral, commercially available, not endorse or favor any particular solution and should allow for technological innovation.

- The marketplace should rely on existing trust infrastructures to provide the equivalence of accreditation where appropriate. If and when the accreditation is considered, the marketplace should determine whether an accreditation or certification of certificate authorities is required. Those that undertake the accreditation or certification of certificate authorities should be held liable for their certification actions. Any accreditation solution should be developed in response to a specific market need and tailored to address a well-defined requirement.

- In order to facilitate electronic transactions across borders, governments should enable the emergence of borderless networks of certification authorities by supporting voluntary non-discrimination agreements. Governments should not impose any licensing or other schemes that could disrupt such non-discrimination.

- Governments should facilitate the emergence of borderless networks of certification authorities by supporting mutual recognition agreements. Governments should not impose any licensing schemes that could disrupt such mutual recognition.

C. Information Compliance

Issue

The legal and regulatory requirements that affect their use of ICT are referred to as "information compliance".

Since the mid-1990s, a significant change in the number, nature and content of ICT-related legal requirements. In addition to the more traditional laws addressing ICT-specific issues (privacy laws, e-contracting laws, e-signature laws etc), requirements affecting companies' ICT deployment are today spreading over many different types of legislation: environment laws, labor laws, tax laws, corporate governance laws, anti-terrorism laws, anti money-laundering laws, sectoral laws, supply chain compliance laws, consumer protection laws, financial stability laws etc.

Forums where this issue is discussed and/or addressed

Professional bodies
Surveillance authorities including for example the US Securities and Exchange Commission

ICC concerns, recommendations and position

Depending upon the way governments impose information compliance requirements, they can either assist businesses in developing better practices or cause severe costs and problems.

Information compliance problems that create significant challenges to business include:

- Obligations frequently differ greatly, and sometimes even conflict, among different regulatory areas and jurisdictions, which can create significant implementation and operational challenges. For instance, companies may be subject to data protection rules in one jurisdiction, which restrict the transfer of personal information across borders, and security requirements in another, which require companies to compile "watch lists" of their global clients.

- The requirements in each country can be difficult to access, and in some cases may even not be set out in writing.

- Often these laws impose serious sanctions; however there is a lack of concrete guidance on how to comply and allowing for companies to avoid such sanctions.

- Businesses increasingly have to understand, monitor and ensure compliance with widely varying ICT-related requirements in numerous different laws in all countries where they are active, as well as in countries that are directly or indirectly affected by their activities.

Principles for constructive legislative practices for information compliance

Governments should work with business to improve awareness of information compliance in the private sector. Moreover, governments should recognize that, in order to be effective, information compliance requirements should be based on the following basic principles:

- Proportionality
- Avoid conflicts
- Technology neutral
- Future-proof
- Standards-informed but not standards-specific
- Mindful of economic impact
- Clear
- Non-discriminatory
- Enforceable
- Flexible
- Pro-competitive
- Pro-trade
- Resources and preparedness
- Period of grace and independent appeal

ICC series on information compliance and governance: Applying ICC's information compliance principles to EU and global debates on e-invoicing

ICC believes it is reasonable that (at least until such time as tax administrations worldwide become more skilled in the evaluation of IT systems and processes) governments can legitimately require businesses to apply security measures that present certain audit advantages, ICC emphasizes that the public/private sector division of cost in relation to such processes should be no different between paper invoicing and electronic invoicing.

Regardless of the specific changes that Europe might make to further refine its legislative framework around e-invoicing, it must be recognized that the global situation concerning electronic invoicing will for the foreseeable future remain characterized by extreme fragmentation of highly complex legal requirements among countries. Intergovernmental cooperation can lower such barriers and eliminate some unnecessary obstacles, however ICC strongly believes that intensified cooperation with the private sector (for example, through the collaborative definition

of international model agreements and good practice guidelines) is more likely to produce balanced and sustainable results within reasonable time-frames. There are many examples of such collaborative private/public sector approaches providing a way forward in areas of significant tension between public policy and business objectives; to mention a few:

- ICC has been one of the leading forces behind the development of the UN-CID Rules, which, even decades ago, became the undisputed basis for the vast majority of successful model EDI agreements worldwide (including the model agreement incorporated in European Commission Recommendation 1994/820/EC).

- More recently, ICC has successfully led the development of model clauses for the protection of personal data in trans-border data flows.

ICC calls on governments and tax administrations to consider the brief observations contained in this paper. Our members, representing companies of all sizes worldwide and from all sectors, would be pleased to work with the public sector in the development of appropriate approaches for the facilitation and effective auditability of electronic invoicing as a cornerstone of seamless global e-business.

SECTION V: Legal Aspects

A. Jurisdiction and Applicable Law

Issue

The Internet and online consumer transactions raise new issues regarding jurisdiction and applicable law in case of a dispute.

Many e-commerce transactions raise questions of compliance with applicable public laws and sectoral regulations. Governments, judiciaries and legislatures are grappling with the question of whose laws apply in cyberspace, and the parties themselves often are unsure of the legal framework within which they are operating.

In many instances, courts are claiming jurisdiction over and applying their countries' laws to websites of companies located outside of their geographic boundaries. Such reach could subject companies to the courts and laws – sometimes conflicting -- of virtually any country from which their website can be accessed.

Forums where this issue is discussed and/or addressed

American Law Institute
Hague Conference
Internet Governance Forum (IGF)
Rome Convention – European institutions

ICC concerns, recommendations and positions

Many companies are not willing to subject themselves to the costs of investigation and compliance with myriad rules in each country, or the risk of sanctions, unenforceable contracts, and adverse publicity around the globe, and are therefore limiting the use of their websites in terms of both products and geography.

Of particular importance is the stifling effect that this would have on SMEs and the severe limitations it would place on emerging entrepreneurial ventures in developing economies.

What's more, some governments have adopted application of the "country-of-destination" principle, which states that the applicable law and jurisdiction are those where the consumer resides in the event of a B2C cross-border dispute. Application of this principle will severely limit greater consumer choice and more favorable prices.

ICC believes that the following principles and strategies will help legislatures, regulatory bodies, and courts in making determinations regarding the complex issues of jurisdiction and choice of law:

- For business to customer e-commerce to reach its full potential, certainty and confidence is essential for both business and consumers when disputes arise between them on-line. ICC believes that the greatest majority of consumer complaints will be resolved either by a company's internal customer service or similar mechanism, or dispute resolution services. However, this does not preclude the need for a predictable legal framework in which to address the few disputes that persist. Therefore, business seeks a predictable and stable framework for resolving these disputes.

- Avoid expansive jurisdictional claims: Governments should take care to avoid creating unpredictable grounds for asserting jurisdiction over e-commerce activities. ICC urges the adoption of the following fundamental principles in order to avoid expansive jurisdictional claims.

    - Party autonomy
    - "Country-of-Origin"
    - Allow self-regulation to demonstrate its efficacy

- The private sector should be given adequate time to assess the market and to develop self-regulatory initiatives, including dispute resolution mechanisms, to resolve these problems. Such initiatives are flourishing as was highlighted at the joint ICC, OECD, and Hague Conference on Private International Law conference on B2C ADR held at The Hague in December 2000.

- Self-regulatory solutions provide the flexibility to respond to the dynamic nature of the online environment. Any policies must accommodate and promote this highly dynamic environment, which is a significant engine of economic growth and social development.

ICC believes that while problems surrounding jurisdiction and applicable law will continue to be studied at national and international levels, the above principles and strategies will assist legislatures, regulatory bodies, and courts to make sound determinations regarding these complex issues.

B. Electronic Contracting

Issue

Creating certainty in the use of electronic contracts

Forums where this issue is discussed and/or addressed

United Nations Commission on International Trade Law (UNCITRAL)

ICC concerns, positions, recommendations

ICC provided input to the development of the UNCITRAL convention on the Use of Electronic Communications in International Contracts, and endorsed it in 2006 at the signing ceremony in July. Moreover, in 2004, ICC developed "eTerms", a set of articles developed by business that parties can incorporate into their contracting document that make it clear they intend to agree to a binding electronic contract. These terms and the UNCITRAL Convention, therefore, complement each other.

Businesses, governments and other users of information and communication technologies have a mutual interest in ensuring that that legal, policy and regulatory frameworks for these technologies are developed with the input of all relevant stakeholders, especially including the private sector. This is the best way to ensure that these technologies will promote investment, foster entrepreneurship, and stimulate innovation. This convention is a positive contribution towards this objective.

Three ways in which this convention will be helpful to businesses, and all users, in the countries that ratifies it.

- First, the UNCITRAL convention allows electronic communications to satisfy the requirements of other international conventions without needing to individually renegotiate each of these conventions.

- Second, ICC welcomed the provisions that require signatory countries to recognize the legal validity of electronic communications used in contracts, as well as those dealing with issues that commonly arise in electronic agreements, such as location of the parties, information and form requirements, time and place of dispatch and receipt of electronic communications, invitations to make offers, and errors.

- Thirdly, ICC welcomed the enhanced legal certainty and support for the concept of party autonomy that the convention provides. The convention allows parties to contracts to shape their electronic agreements in the most productive way possible, and it supplies the legal foundation for the parties to ensure that their electronic contract meets their specific needs.

SECTION VI: ICT: regulatory and market issues

A. Open source software

Issue

Open source software — as a software development and licensing model—is an emerging business reality. Open source software (OSS) refers to software for which the underlying "source" code available for inspection and modification by anyone interested in doing so; subject, possibly (depending on the exact details of the license), adherence to any licensing requirements. This contrasts to proprietary software, the source code for which is often not made available to third parties. The term "open source" is often applied in two distinct ways: (1) to a software programme licensed under particular terms and (2) to a software development model.

The global software market employs millions of people and generates turnover of hundreds of billions of $US; Open source software forms a crucial part in this market place. One can, for example, refer to: LINUX operating system and Apache HTTP Server Project, both software tools having millions of users.

Open source and proprietary software both play an important role in the global software marketplace. Open source and proprietary software operate under different 'licensing' models.

National governments should recognize the distinction between these licensing models.

Forums where this issue is discussed and/or addressed

National governments

ICC concerns, positions and recommendations

Procurement leaders in government and industry should consider many factors when acquiring software. Many of these factors apply independent of the 'licensing model'.

These key questions are:

- Does the functionality of the software meet business needs?
- What is the total cost of customizing, managing and improving the software?
- What services are provided to maintain, modify and customize the software?
- How interoperable is the software with other software?
- How secure is the software?
- Has the software been independently security evaluated?

Open standards" and "open source software"

"Open standards" are publicly available technical specifications. Whilst there exist no definition of the 'standards' some standards do develop by consensus in the market place. Additionally, some standards are developed by "Standards Settings Organizations" and subject to the individual rights of those standards / licenses.

"Open source software" is not the same as "Open standards". Whether a 'standard' has been defined as 'open' or not has nothing to do with the licensing model or any terms attached to the software. 'Open standards' merely indicate that the technical specifications are documented in a manner which allows that products can be created to interact with 'open standard' software of the same technical description.

"Open source" software, of course, means that the entire source code (software) is publicly available for analysis / scrutiny.

Public policy implications of Open Source Software

- Procurement preferences

ICC opposes government procurement preferences and mandates that favor one form of software development or licensing over others. Governments, like all potential and existing customers, should choose software on a technology-neutral and vendor-neutral basis, examining the merits of the technology based upon the performance factors stated above. As a general rule, governments should not discriminate against or ban the procurement of software based on its licensing or development model. Such preferential policies prevent public authorities from effectively weighing all relevant factors in their procurement decisions.

- Intellectual property concerns

Regardless of development model, the software industry relies on intellectual property law. Effective government intellectual property frameworks are important to commercial and open source development models. Both models rely on intellectual property protection to safeguard software programmes and allow products to be used by the community or sold to customers. Intellectually property rights frameworks create an effective environment for open source and commercial software firms to invest resources into creating new products and technologies. All participants in the software industry are well served by government policies that create robust and transparent enforcement mechanisms of intellectual property rights for software.

The combination of open source and proprietary development and licensing models yields a dynamic and innovative software industry while providing users with many choices to meet their needs. No one licensing or development model is appropriate for all customers or users in all situations. ICC believes the best mechanisms for governments to support innovation and the software industry are policies where no blanket preferences are provided based solely on the licensing or development model and supports continued and enhanced funding for basic software research coupled with effective and transparent intellectual property protection.

B. Mandatory certification requirements for IT products and services

Issue

The increasing globalization of business and expanding regulation of commerce by states have led to a significant rise in the extraterritorial application of national laws, with states frequently applying or seeking to apply their laws and regulations to persons or conduct outside national borders.

Mandatory certification requirements that impose overly burdensome requirements risk restricting market access, creating barriers to trade, and imposing untenable data privacy and security requirements. Such certification requirements place an undue burden on business, may create disincentives for local investment in plants and operations, and can negatively impact the global economy.

Mandatory certification requirements for IT products and services at national level should be consistent with international norms and regulations, based on voluntary international standards such as those of the International Organization for Standardization (ISO).

Forums where this issue is discussed and/or addressed

National governments
Telecommunication Standardization Sector (ITU-T)

ICC concerns, positions, recommendations

ICC is strongly committed to promoting cross-border investment and trade as indispensable elements of sustainable economic development and world growth. An overall objective of business and government trade policy should be to reduce or eliminate non-tariff barriers, where these reductions would contribute to further liberalization. National regulatory regimes should avoid creating unintended trade barriers which can lead to a fragmented global market and protectionism.

Mandatory certification programmes that are not aligned with international standards often create more problems than they resolve and do not take into account the wealth of international consensus-based information security standards that exist to address these issues. Thus, information technology (IT) product and services certification programmes/initiatives should be based on and consistent with internationally accepted voluntary standards and norms.

Foreign companies may otherwise be disadvantaged in obtaining the required algorithms and documentation to make products comply with the nationally based regulation not based on international standards. Local requirements should be recognized in international standards fora, where they can be properly vetted, and – if adopted- where the requirements will be publicly available on an equal basis.

Compliance assessment can then take many forms and when implemented consistently will not become a barrier, such as various concerns below:

Predictability

Clear and predictable rules of law are essential to achieve these objectives.

Conflicting requirements

Extraterritoriality increases tensions among governments, stemming both from disagreements by states on the means of regulating activity or the policies underlying extraterritorial measures and from discord in addressing such conflicts.

Increased economic costs

The extraterritorial application of national laws affects companies of all sizes and across industries. It increases international transaction costs for companies and may result in steep compliance and regulatory costs.

Innovation

Product certification initiatives that go beyond international standards may damage the competitiveness and opportunities for countries that adopt them if new and innovative products and technologies will not be made available in such markets.

Competitiveness

Maintaining a host of different product versions to comply with different local regimes will add to the cost of doing business and it will make products more expensive for consumers and less available in local markets.

Intellectual Property (IP) Rights

Mandatory certification requirements could also directly impact companies by imposing substantial cost burdens to produce products for the global market and separate product lines for a specific market.

Forced Intellectual Property Rights Transfer

This is a real concern for business, and requirements to disclose confidential source code, for example, and other documentation to comply with national certification initiatives create technical barriers to trade. Harmonized control processes should be encouraged.

ANNEX

I. What is Business Action to Support the Information Society (BASIS)?

ICC created BASIS to serve as the voice of business in the global dialogue on the Information Society, following the two World Summits on the Information Society (WSIS) held in Geneva (2003) and Tunis (2005). BASIS participates in UN-linked forums set up to continue the dialogue, such as the Internet Governance Forum (IGF), the Global Alliance for ICT and development (GAID) and the WSIS follow-up and implementation processes.

BASIS builds on the activities and network of the Coordinating Committee of Business Interlocutors (CCBI), which ICC formed to coordinate participation by world business in the processes leading up to and at the Summits in Geneva and Tunis.

To promote the environment in which global business will continue to thrive as an innovator of these technologies, BASIS mobilizes business to help shape the agenda and participate in these global discussions. The initiative aims to unite the business community, to raise awareness among the public, governments, civil society, intergovernmental organizations and technical authorities of what business requires continuing contributing to the development of the Information Society. BASIS relies on policies developed in ICC's Commission on E-business, IT and Telecoms (EBITT) as the foundation for its efforts.

For further information regarding BASIS, the founding partners, members and activities, please consult the BASIS website at: www.iccwbo.org/basis

II. Overview of Forums

Asia-Pacific Economic Cooperation (APEC)

Asia-Pacific Economic Cooperation (APEC) works in three broad areas to meet the Bogor Goals of free and open trade and investment in the Asia-Pacific by 2010 for developed economies and 2020 for developing economies.

Known as APEC's 'Three Pillars', APEC focuses on three key areas:

- Trade and Investment Liberalization
- Business Facilitation
- Economic and Technical Cooperation

The outcomes of these three areas enable APEC Member Economies to strengthen their economies by pooling resources within the region and achieving efficiencies. Tangible benefits are also delivered to consumers in the APEC region through increased training and employment opportunities, greater choices in the marketplace, cheaper goods and services and improved access to international markets.

For more information about APEC, its member economies and work program please consult: www.apecsec.org.sg

Council of Europe

The Council of Europe is an international organization of 47 member states in the European region (with Azerbaijan, Armenia, Turkey, Georgia and Cyprus also extending into Western Asia and Russia into North Asia.) With the exception of Belarus and Kazakhstan all European states have acceded to the Council of Europe. Canada, Japan, Mexico, the USA and the Holy See have Observer Status with the Council of Europe and the parliaments of Canada, Israel and Mexico have observer status with its Parliamentary Assembly. NGOs can participate in the INGO Conference of the Council of Europe. Several conventions of the Council of Europe have also been signed by non-European states, for example the Convention on Cyber crime, the Anti-Doping Convention and the Bern Convention for the Protection of Natural Habitats.

Its most enduring legacy is the European Convention on Human Rights, adopted in 1950, which serves as the basis for the European Court of Human Rights. English and French are its two official languages, but its Committee of Ministers and its Parliamentary Assembly also work in German, Italian and Russian.

The seat of the Council of Europe is in Strasbourg on the Franco-German border. Originally meeting in Strasbourg's University Palace, it is now domiciled in the Palace of Europe about two kilometers from city centre. Membership is open to all European democracies which accept the principles of the rule of law and are able and willing to guarantee fundamental human rights and freedoms.

The Council of Europe should not be confused with the Council of the European Union or the European Council, as it is a separate organization and not part of the European Union which, however, adopted the same European flag and anthem.

For more information about the Council, please consult: www.coe.int/DefaultEN.asp

European Commission

The European Commission is the executive branch of the European Union. It operates as a cabinet government with 27 Commissioners led by a Commission President (currently José Manuel Barroso). There is one Commissioner per member state, though Commissioners are bound to represent the interests of the EU as a whole rather than their home state. One of the 27 is the Commission President (currently José Manuel Durão Barroso) appointed by the European Council. The first Barroso Commission took office in late 2004 and its successor, under the same President, took office in 2010. The body is responsible for proposing legislation, implementing decisions, upholding the Union's treaties and the general day-to-day running of the Union

The term "Commission" can mean either the college of Commissioners mentioned above, or the larger institution; including the administrative body of about 23,000 European civil servants who are divided into departments called Directorates-General. It is primarily based in the Berlaymont building of Brussels and its internal working languages are English, French and German.

The Commission was set up from the start to act as an independent supranational authority separate from governments; it has been described as "the only body paid to think European". Although the members come from national governments, they are bound to act independently — neutral from other influences. This is in contrast to the Council, which represents governments, and the Parliament, which represents citizens.

The Commission is primarily based in Brussels, in the Berlaymont. The President's office and the Commission's meeting room are based on the 13th floor. The Commission also operates out of numerous other buildings in Brussels and Luxembourg. The Commission is divided into departments known as Directorates-General (DGs) that can be likened to departments or ministries. Each covers a specific policy area or service such as External relations or Translation. Each DG is headed by Director-General who is responsible to a Commissioner. A Commissioner's portfolio can be supported by numerous DGs. DGs prepare proposals and if adopted by a majority of Commissioners when meeting it goes forward to Parliament and Council for consideration.

For more information about the Commission, please consult: ec.europa.eu/index_en.htm

The U.N. Global Alliance for Information and Communication Technologies and Development (GAID)

An initiative approved by the United Nations Secretary-General in 2006, was launched after comprehensive worldwide consultations with governments, the private sector, civil society, the technical and Internet communities and academia.

While the 2005 United Nations Summits emphasized the importance of ICT in achieving the internationally agreed development goals, including the Millennium Development Goals (MDGs), there was a need for a truly global forum that would comprehensively address cross-cutting issues related to ICT in development.

Recognizing that no single actor is capable of achieving the MDGs in isolation, the creation of an open and inclusive platform that can broaden the dialogue on innovative ways of harnessing ICT for advancing development is crucial.

The Global Alliance is a direct response to this need. With its multi-stakeholder approach, the Alliance reaffirms the belief that a people-centered and knowledge-based information society is essential for achieving better life for all.

For more information about GAID, please consult: www.un-gaid.org

Hague Conference on Private International Law

The Hague Conference on Private International Law ("the Hague Conference") is a leading organization in the area of private international law. Founded in 1893, its purpose has been to "work for the progressive unification of the rules of private international law". It has pursued this goal by creating and assisting in the implementation of multilateral conventions promoting the harmonization of conflict of laws principles in diverse subject matters within private international law. Sixty-five nations are currently members of the Hague Conference, including China, Russia, the United States, and all member states of the European Union.

The most recent convention concluded by the Hague Conference is the Hague Convention on Choice of Court Agreements, of 30 June 2005, applicable certain B2B international contracts that include provisions on choice of forum.

For more information about The Hague Conference or the Convention on Choice of Court Agreements, please consult: www.hcch.net/index_en.php

Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function.

As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

ICANN is responsible for coordinating the management of the technical elements of the Domain Name System (DNS) to ensure universal resolvability so that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique technical identifiers used in the Internet's operations, and delegation of Top-Level Domain names (such as .com, .info, etc.).

Other issues of concern to Internet users, such as the rules for financial transactions, Internet content control, unsolicited commercial email (spam), and data protection are outside the range of ICANN's mission of technical coordination.

Participation in ICANN is open to all who have an interest in global Internet policy as it relates to ICANN's mission of technical coordination. ICANN provides many online forums which are accessible through ICANN's website, and the Supporting Organizations and Advisory Committees have active mailing lists for participants. Additionally, ICANN holds public meetings throughout the year.

For more information about the ICANN, please consult: www.icann.org

The Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC3935.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. IETF meetings are held three times a year.

The IETF working groups are grouped into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB.

For more information about IETF, please consult: www.ietf.org

Internet Governance Forum (IGF)

The Tunis Agenda for the Information Society signed at the second phase of the World Summit on the Information Society (WSIS, Tunis 2005) invited the Secretary-General of the United Nations to convene a new forum for multi-stakeholder policy dialogue, called the Internet Governance Forum [IGF], by the second quarter of 2006 and to implement this mandate in an open and inclusive process.

The first IGF took place in Athens, Greece from 30 October to 2 November 2006. The next IGF event took place in Rio de Janeiro, Brazil from 12 to 15 November 2007. The third IGF took place in Hyderabad, India from 3 to 6 December 2008 and the fourth IGF took place in Sharm el-Sheikh, Egypt from 15 to 18 November 2009. The fifth IGF will take place in Vilnius, Lithuania from 14 to 17 September 2010.

For more information about the Internet Governance Forum, please consult:
www.intgovforum.org

Internet Protocol Version 6 Forum (IPv6 Forum)

The IPv6 Forum is a world-wide consortium of worldwide leading Internet vendors, Industry Subject Matter Experts, Research & Education Networks, with a clear mission to advocate IPv6 by dramatically improving technology, market, and deployment user and industry awareness of IPv6, creating a quality and secure new Generation Internet and allowing world-wide equitable access to knowledge and technology, embracing a moral responsibility to the world.

To this end the IPv6 FORUM has:

- Established an open, international FORUM of IPv6 expertise
- Shared IPv6 knowledge and experience among members
- Promoted new IPv6-based applications and global solutions
- Promoted interoperable implementations of Ipv6 standards
- Co-operated to achieve end-to-end quality of service
- Resolved issues that create barriers to IPv6 deployment

The Internet Engineering Task Force has sole authority for IPv6 protocol standards. The IPv6 Forum reserves the right to develop IPv6 Deployment Guides to foster the operational use of IPv6. The IPv6 Forum is a non-profit organization registered in Luxembourg since July 17, 1999. The admin secretariat is run by the audit company Horsburgh based in Luxembourg.

For more information about IPv6 Forum: www.ipv6forum.com

International Telecommunication Union (ITU)

The ITU is the leading United Nations agency for information and communication technologies. As the global focal point for governments and the private sector, ITU's role in helping the world communicate spans 3 core sectors: radio communication, standardization and development. ITU also organizes TELECOM events and was the lead organizing agency of the World Summit on the Information Society.

The ITU has developed, under the Digital Opportunity Platform, the Digital Opportunity Index (or DOI) as a tool to measure the Information Society. DOI is a composite index based on 11 core ICT indicators. The structure of the index is sequential, which makes it more flexible and allows to use it in combination with other existing indices (such as the UNDP Human Development Index) The DOI was endorsed by the World Summit on the Information Society in the Tunis Agenda for the Information Society as a tool for mapping of digital opportunity worldwide.

ITU is based in Geneva, Switzerland, and its membership includes 191 Member States and more than 700 Sector Members and Associates.

Members are the Vatican City and almost all of the UN members. Only Palau and East Timor are not participating. Other entities not represented are the Palestinian Authority, Taiwan and the Saharawi Republic (Western Sahara).

The ITU decides matters between states and private organizations through an extensive series of working parties, study groups, regional meetings, and world meetings.
Examples:

- World Radio communication Conference
- World Administrative Radio Conference
- Regional Radio telecommunications Conferences.

For more information about ITU, please consult: www.itu.int/en/pages/default.aspx

Organization for Economic Co-operation and Development (OECD)

The OECD groups 30 member countries sharing a commitment to democratic government and the market economy. With active relationships with some 70 other countries and economies, NGOs and civil society, it has a global reach. Best known for its publications and its statistics, its work covers economic and social issues from macroeconomics, to trade, education, development and science and innovation.

The OECD plays a prominent role in fostering good governance in the public service and in corporate activity. It helps governments to ensure the responsiveness of key economic areas with sectoral monitoring. By deciphering emerging issues and identifying policies that work, it helps policy-makers adopt strategic orientations. It is well known for its individual country surveys and reviews .

The OECD produces internationally agreed instruments, decisions and recommendations to promote rules of the game in areas where multilateral agreement is necessary for individual countries to make progress in a globalized economy. Sharing the benefits of growth is also crucial as shown in activities such as emerging economies, sustainable development, territorial economy and aid.

Dialogue, consensus, peer review and pressure are at the very heart of OECD. Its governing body, the Council, is made up of representatives of member countries. It provides guidance on the work of OECD committees and decides on the annual budget. It is headed by Angel Gurría, who took up the post of Secretary-General on 1 June 2006.

For more information about the OECD, please consult www.oecd.org

The United Nations Commission on International Trade Law (UNCITRAL)

The United Nations Commission on International Trade Law (UNCITRAL) is a body of member and observer states under the auspices of the United Nations.

The Commission is composed of sixty member States elected by the General Assembly. Membership is structured so as to be representative of the world's various geographic regions and its principal economic and legal systems. Members of the Commission are elected for terms of six years, the terms of half the members expiring every three years.

The Commission carries out its work at annual sessions, which are held in alternate years at United Nations Headquarters in New York and at the Vienna International Centre at Vienna. Each working group of the Commission typically holds one or two sessions a year, depending on the subject-matter to be covered; these sessions also alternate between New York and Vienna.

In addition to member States, all States that are not members of the Commission, as well as interested international organizations, including the ICC, are invited to attend sessions of the Commission and of its working groups as observers. Observers are permitted to participate in discussions at sessions of the Commission and its working groups to the same extent as members.
The Commission has established six working groups to perform the substantive preparatory work on topics within the Commission's programme of work. Each of the working groups is composed of all member States of the Commission.

- Working Group IV – Electronic Commerce – (recent work products include the model law on e-commerce, e-signatures, and the e-contracting convention

For more information about the Commission, please consult:
www.uncitral.org/uncitral/en/index.html

World Summit on the Information Society (WSIS Geneva 2003, Tunis 2005)

The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis, from 16 to 18 November 2005.

WSIS Geneva: 10-12 December 2003

The objective of the first phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake.

Nearly 50 Heads of state/government and Vice-Presidents, 82 Ministers, and 26 Vice-Ministers from 175 countries as well as high-level representatives from international organizations, private sector, and civil society attended the Geneva Phase of WSIS and gave political support to the Geneva Declaration of Principles and Geneva Plan of Action that were adopted on 12 December 2003. More than 11,000 participants from 175 countries attended the Summit and related events.

WSIS Tunis: 16-18 November 2005

The objective of the second phase was to put Geneva's Plan of Action into motion as well as to find solutions and reach agreements in the fields of Internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents.

Nearly 50 Heads of state/government and Vice-Presidents and 197 Ministers, Vice Ministers and Deputy Ministers from 174 countries as well as high-level representatives from international organizations, private sector, and civil society attended the Tunis Phase of WSIS and gave political support to the Tunis Commitment and Tunis Agenda for the Information Society that were adopted on 18 November 2005. More than 19,000 participants from 174 countries attended the Summit and related events.

For more information and full texts of the Geneva and Tunis outcome documents, please consult: www.itu.int/wsis

Principals of the World Summit on the Information Society (WSIS) host countries, Switzerland and Tunisia and the executive secretariat invited the International Chamber of Commerce (ICC) to create the **Coordinating Committee of Business Interlocutors (CCBI)** as a vehicle through which to coordinate the involvement of worldwide business in the processes leading to and culminating in the WSIS in Geneva 2003 and Tunis 2005. The CCBI was made up of – and open to all – representatives of individual business firms, as well as of associations and other organizations that represent business interests. The regional diversity of CCBI members ensured that its views were truly global.

For archived information regarding the CCBI and its activities and inputs throughout the preparations for both phases of the WSIS and at the Summits themselves, please consult: www.iccwbo.org/businessatwsis

The World Trade Organization (WTO)

The World Trade Organization (WTO) is an international organization designed to supervise and liberalize international trade. The WTO came into being on January 1 1995, and is the successor to the General Agreement on Tariffs and Trade (GATT).

The World Trade Organization deals with the rules of trade between nations at a near-global level; it is responsible for negotiation and implementing new trade agreements, and is in charge of policing member countries' adherence to all the WTO agreements, signed by the current work comes from the 1986-94 negotiations called the Uruguay Round and earlier negotiations under the GATT. The organization is currently the host to new negotiations, under the Doha Development Agenda (DDA) launched in 2001.

The WTO is governed by a Ministerial Conference, which meets every two years; a General Council, which implements the conference's policy decisions and is responsible for day-to-day administration; and a director-general, who is appointed by the Ministerial Conference. The WTO's headquarters are in Geneva, Switzerland.

The WTO's stated goal is to improve the welfare of the peoples of its member countries, specifically by lowering trade barriers and providing a platform for negotiation of trade. Its main mission is "to ensure that trade flows as smoothly, predictably and freely as possible". This main mission is further specified in certain core functions serving and safeguarding five fundamental principles, which are the foundation of the multilateral trading system

Among the various functions of the WTO, these are regarded by analysts as the most important:

- It oversees the implementation, administration and operation of the covered agreements.
- It provides a forum for negotiations and for settling disputes.

Additionally, it is the WTO's duty to review the national trade policies, and to ensure the coherence and transparency of trade policies through surveillance in global economic policy-making. Another priority of the WTO is the assistance of developing, least-developed and low-income countries in transition to adjust to WTO rules and disciplines through technical cooperation and training. The WTO is also a center of economic research and analysis: regular assessments of the global trade picture in its annual publications and research reports on specific topics are produced by the organization. Finally, the WTO cooperates closely with the two other components of the Bretton Woods system, the IMF and the World Bank.

For more information about the WTO, please consult: www.wto.org

The International Chamber of Commerce

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The fundamental mission of ICC is to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the last century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rules-setting, dispute resolution and policy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on vital technical and sectoral subjects. These include financial services, information technologies, telecommunications, marketing ethics, the environment, transportation, competition law and intellectual property, among others.

ICC enjoys a close working relationship with the United Nations and other intergovernmental bodies, including the World Trade Organization and the G8.

ICC was founded in 1919. Today it groups hundreds of thousands of member companies and associations from over 120 countries. National committees work with their members to address the concerns of business in their countries and convey to their governments the business views formulated by ICC.

For information on how to join ICC, visit the ICC website **(iccwbo.org)** or contact the ICC Membership Department in Paris.

International Chamber of Commerce
The world business organization
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 28 59
E-mail icc@iccwbo.org Website www.iccwbo.org