



3rd edition

A Global Action Plan for Electronic Business

**Prepared by Business with
Recommendations for Governments**

July 2002

Collectively, the Alliance for Global Business represents the following organizations;

Arbeitsgemeinschaft für Datenverarbeitung (ADV), Austria	ICC Argentina
Asociácia Zamestnávateľ'skych Zväzov a Združení Slovenskej Republiky, Slovak Republic	ICC Australia
Asociación Española de Empresas de Tecnologías de la Información (SEDISI), Spain	ICC Austria
Asociación Mexicana de la Industria de Tecnologías de Información (AMITI), Mexico	ICC Bahrain
Associação Industrial Portuguesa (Portuguese Industrial Association)	ICC Bangladesh
Associação Portuguesa das Empresas de Tecnologias de Informação e Comunicações (APESI), Portugal	ICC Belgium
Association for Consulting to Business (APP), Czech Republic	ICC Brazil
Association Française des Utilisateurs du Téléphone et des Télécommunications, (AFUTT)	ICC Burkina Faso
Association of Telecommunication Users (AUTEL), Spain	ICC Cameroon
Association of the Computer Industry (PIKOM), Malaysia	ICC Canada
Association Suisse d'Usagers de Télécommunications, (ASUT)	ICC Chile
Associazione Nazionale Aziende Servizi Informatica e Telematica Italy	ICC China
Associazione Nazionale Utenti Italiani di Telecomunicazioni (ANUIT)	ICC Colombia
Australian Chamber of Commerce and Industry	ICC Costa Rica
Australian Information Industry Association (AIIA)	ICC Cuba
Australian Telecommunications Users Group (ATUG)	ICC Czech Republic
Bangladesh Computer Samity (BCS)	ICC Cyprus
Belgian Telecommunications Users Group (BELTUG)	ICC Denmark
Bundesverband der Deutschen Industrie (Federation of German Industries)	ICC Ecuador
Bundesverband Informationstechnologien (BVITeV), Germany	ICC Egypt
Bundesvereinigung der Deutschen Arbeitgeberverbände (Confederation of German Employers' Associations)	ICC Finland
Cámara de Empresas de Software y Servicios Informáticos (CESSI), Argentina	ICC France
Canadian Council for International Business	ICC Germany
CEHIC (Confederation of Hungarian Employers' Organisations for International Cooperation)	ICC Ghana
Colombian Software Federation (FEDECOLSOFT)	ICC Greece
Communications Users Association of South Africa (CUASA)	ICC Hungary
Computer Suppliers' Association of Zimbabwe (COMSA)	ICC Iceland
Computing Services & Software Association (CSSA), UK	ICC India
Confederacion de Camaras Industriales de los Estados Unidos Mexicanos (CONCAMIN) (Mexican Confederation of Chambers of Industry)	ICC Indonesia
Confederacion Espanola de Organizaciones Empresariales (Spanish Confederation of Employers' Organizations)	ICC Iran (Islamic Republic of)
Confederacion Patronal de la República Mexicana (COPARMEX) (Employers Confederation of the Mexican Republic)	ICC Ireland
Confederation of British Industry	ICC Israel
Confederation of Industry of the Czech Republic	ICC Italy
Confederazione Generale dell'Industria Italiana (General Confederation of Italian Industry)	ICC Japan
Dansk Arbejdsgiverforening (Danish Employers' Confederation)	ICC Jordan
Dansk Dataforening (DDF), Denmark	ICC Korea
Dansk Industri (Confederation of Danish Industries)	ICC Kuwait
Electronic Commerce Association of South Africa (ECASA)	ICC Lebanon
Fédération des Entreprises de Belgique (Federation of Belgian Industry - FEB-VBO)	ICC Lithuania
Fédération des Industriels Luxembourgeois (Federation of Luxembourg Industrialists)	ICC Luxembourg
Federation of Dutch Branch Associations in Information Technology (FENIT)	ICC Monaco
Federation of Hellenic Information Technology Enterprises (SEPE)	ICC Mongolia
Federation of Korean Industries (FKI)	ICC Mexico
Federation of Korean Information Industries (FKII)	ICC Morocco
Hong Kong Information Technology Federation (HKITF)	ICC Netherlands
Hong Kong Telecommunications Users Group (HKTUG)	ICC Nepal
ICC Algeria	ICC New Zealand
	ICC Nigeria
	ICC Norway
	ICC Pakistan
	ICC Poland
	ICC Peru
	ICC Philippines
	ICC Portugal
	ICC Qatar
	ICC Romania
	ICC Russia
	ICC Saudi Arabia
	ICC Senegal
	ICC Singapore
	ICC Slovakia
	ICC Slovenia
	ICC South Africa
	ICC Spain
	ICC Sri Lanka
	ICC Sweden
	ICC Switzerland
	ICC Syria
	ICC Tanzania

ICC Thailand
 ICC Togo
 ICC Tunisia
 ICC Turkey
 ICC Ukraine
 ICC United Kingdom
 ICC Uruguay
 ICC Venezuela
 ICC Yugoslavia
 ICC Caribbean
 Chinese Taipei Business Council of ICC
 Hong Kong, China Business Council of ICC
 Information Service Industry Association of China, Taipei (CISA) China
 Information Technology Association of America (ITAA)
 Information Technology Association of Canada (ITAC)
 Information Technology Association of New Zealand (ITANZ)
 Information Technology Services Association (TIPAL), Finland
 International Communication User Group (ICUG), Ireland
 International Communications Association (ICA), USA
 International Press Telecommunications Council (IPTC)
 Irish Business and Employers Confederation (IBEC)
 Israeli Association of Software Houses (IASH)
 IT Association of South Africa (ITA)
 IT&C Association of Romania (ATIC)
 Japan Information Service Industry Association (JISA)
 Keidanren - BIAJ Japan (Federation of Economic Organizations)
 Konfederacja Pracodawcow Polskich (Confederation of Polish Employers)
 L'Association des Professionnels de L'Informatique de la Bureautique et de la Telematique (APEBI), Morocco
 Mongolian National Information Technology Association
 Mouvement des Entreprises de France (MEDEF) (French Enterprises Association)
 Næringslivets Hovedorganisasjon (Confederation of Norwegian Business and Industry)
 Näringslivets Telekommitté (NTK), Sweden
 National Association of Software and Service Companies (NASSCOM), India
 Nederlandse vereniging van bedrijfs telecommunicatie grootgebruikers (BTG)
 Business New Zealand
 Norsk Tele- og Informasjonsbrukerforening (NORTIB)
 Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji - PIIT)

SA Value Added Network Services Association (SAVA), South Africa
 Samtök Atvinnulífsins, Iceland
 Singapore Information Technology Federation (SITF)
 Slovenská Obchodná a Priemyselná Komora Slovak Republic
 Sociedade de Usuários de Informática e Telecomunicações - Sao Paulo (SUCESU-SP), Brazil
 Software Industry Federation in Northern Ireland (SIF)
 Sdružení uživatelů elektronických domácností (SUEK) Czech Republic
 Sveskt Näringsliv (Sweden)
 Swedish IT-companies' Organisation AB, Sweden
 Syndesmos Ellinikon Viomichanion (Federation of Greek Industries)
 Syntec Informatique, France
 Telecom eV, Germany
 Telecom Forum Africa Ltd
 Telecommunications Managers Association (TMA), UK
 Telecommunications Users Association (TUA), UK
 Telecommunications Users Association of New Zealand (TUANZ)
 Teollisuuden Ja Työntantajain Keskusliitto (Confederation of Finnish Industry and Employers)
 The Association of Lithuania's Information, technology, telecommunications and office equipment (INFOBALT)
 The Association of Thai Computer Industry (ATCI)
 The Co-operative Society for Computers of Egypt (CSCE)
 Türk Sanayicileri ve İşadamları Derneği (TÜSIAD - Turkish Industrialists' and Businessmen's Association)
 Türkiye İşveren Sendikaları Konfederasyonu (TİSK Turkish Confederation of Employer Associations)
 Türkiye Ticaret - Sanayi - Deniz Ticaret Odaları ve Borsaları Birliği (TOBB - Union of Chambers of Commerce, Industry, Maritime Commerce and Commodity Exchanges of Turkey)
 Union Patronale Suisse (Confederation of Swiss Employers) economiesuisse, Switzerland
 United States Council for International Business (USCIB)
 Industriellenvereinigung (Federation of Austrian Industry)
 Vereinigung von TK-netzbetreibern des Finanzsektors (VTF), Austria
 Vereniging VNO-NCW (Confederation of Netherlands Industry and Employers VNO-NCW)

This Action Plan is supported by:

World Association of Newspapers (WAN)
World Economic Forum (WEF)
World Federation of Advertisers (WFA)
World Trade Centres Association (WTCA)
International Express Carriers Conference (IECC)
International Federation of Freight Forwarders' Associations (FIATA)
Eurobit
Eurocommerce
European Community Shipowners' Association (ECSA)
European Society for Opinion and Marketing Research (ESOMAR)
Federation of European Direct Marketing (FEDMA)
Japan-US Business Council
US-Japan Business Council
Advertising Agencies' Association of New Zealand
Advertising Standards Authority New Zealand
Canadian Chamber of Commerce
Canadian Council for International Business (CCIB)
Chamber of Commerce and Industry – Haifa and Northern Israel
German Association of Chambers of Commerce and Industry (DIHT)
Association of New Zealand Advertisers
Information Technology Association of Canada (ITAC)
Keidanren
New Zealand Chambers of Commerce
New Zealand Direct Marketing Association
Pacific Basin Economic Council (PBEC)
Pacific Economic Cooperation Council (PECC) TIIF
The British Phonographic Industry Ltd (BPI)
US Council for International Business (USCIB)

In cooperation with:

**Association Européenne pour la Protection des Oeuvres et services
Cryptés (AEPOC)**
Internet Law and Policy Forum (ILPF)

Table of contents

A Global Action Plan for Electronic Business Prepared by Business with Recommendations for Governments

Introduction to the third edition.....	7
Background.....	7
This document	8
Fundamental principles	9
An Action Plan	10
1. Maximizing the benefits – economic and social impacts.....	10
Economic and social impacts	13
Small and medium-sized enterprises	13
Skills development	14
Ensuring global participation	14
Infrastructure deployment	15
Government as model user	15
2. Electronic business and the information infrastructure – trade aspects, standards, and Internet names and numbers	16
Competition and trade-related aspects of electronic commerce.....	16
Telecommunications competition	16
IT equipment	17
Trade-related aspects of electronic commerce	18
Trade-related aspects of intellectual property	19
Convergence.	19
Standards	20
Internet names and numbers.....	21
Domain name system	21
3. Building trust for users and consumers.....	22
Protection of personal information.....	22
Privacy and transborder flows of data.....	22
Internet privacy.....	23
Consumer trust and content.....	24
Consumer trust	25
Online Alternative Dispute Resolution (ADR)	26
Content	27
Marketing and advertising ethics.....	28
Unsolicited commercial communications	29
Issues relating to cybersecurity	30
Promotion of technology and services development to ensure security.....	30
Cryptography for confidentiality.....	31
Information sharing	31
Cybercrime	32

	Business monitoring of its own communications and networks	33
	Data storage requirements	33
	Searches and subpoenas of computer records	34
	Access to public domain information.....	34
	Legal government interception of telecommunications and electronic communications	34
	Electronic authentication	35
	Legal validity of electronic signatures; interoperability of certificates and electronic signatures.....	35
	Accreditation	37
	Availability of certification practice statements.....	37
4.	Establishing ground rules for the digital marketplace	38
	Contractual and other legal issues	38
	Removing legal/regulatory obstacles	38
	Create a new uniform legal framework.....	39
	Jurisdiction and applicable law	39
	Incorporation by reference	40
	Transparency and availability of proprietary and best practice legal terms, model contracts etc	40
	Dispute settlement	40
	Fraud and other commercial crime.....	40
	Liability	41
	Taxation and tariffs.....	42
	Customs duties	43
	Taxation.....	44
	Trade facilitation and customs modernization	45
	Private/public sector interface	45
	Customs modernization.....	45
	Capacity building.....	46
	Intellectual property.....	47
	Copyright and neighbouring rights.....	47
	Trademarks	48
	Databases	48
IV.	Annex - selected industry self-regulatory initiatives.....	49

1. Introduction to the third edition

Background

This third edition of the Global Action Plan for Electronic Business published by the Alliance for Global Business (AGB) reflects a number of developments in the global discussions about electronic business since the first Global Action Plan was submitted on behalf of business to the OECD Ministerial in Ottawa, Canada, in October 1998. It also responds to a commitment that the AGB made in Ottawa on behalf of business globally to submit evidence, after one year, that the various business actions set forth in the Global Action Plan were being properly implemented.

In its first edition, the Global Action Plan urged governments to rely on business self-regulation and the voluntary use of empowering technologies as the main drivers behind the creation of trust across the whole spectrum of users and providers of e-commerce goods and services. It also stated that governments should focus on the provision of a stable and predictable environment enabling the enforcement of electronic contracts, the protection of intellectual property and safeguarding competition. Furthermore, the Action Plan provided a detailed overview of which issues were the respective responsibilities of the private and the public sectors, and included an exemplary selection of self-regulatory projects.

The organizations in the AGB and the many Action Plan supporters believe that implementation of the business agenda expressed in the Action Plan is progressing satisfactorily. As this update shows, in many areas there is strong evidence that business is responding to the new environment by providing unprecedented transparency and safeguards for consumers. Sometimes the results of such business action can be easily quantified, but more often it is reflected in the figures showing a rapid expansion of e-business globally.

Self-regulation is not a new phenomenon. Throughout history, business has set its own standard rules and practices through a variety of organizations to lower transaction costs, to avoid and resolve conflicts, and to create consumer confidence.

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

This document...

Part II of this document establishes a set of fundamental principles as the basis for the framework in which policymaking for electronic commerce should take place.

Part III presents a proposed framework for action that has been agreed to by the world's leading international business organizations that are working together to provide business leadership, in cooperation with governments and others. The plan describes business actions and commitments in concrete terms and identifies business expectations of government action. It is proposed as a reference point for all relevant business and government organizations to contribute to the efficient and transparent development of the minimal rules necessary for a stable and predictable electronic commerce environment.

The action plan calls for a “hands off” approach by government on certain issues, whilst recognizing that electronic business raises many important public policy considerations that may require governmental facilitation. Government intervention may be required in such matters as intellectual property protection, taxation, and the removal of barriers to competition in providing the underlying infrastructure. However, in other matters, business solutions such as self-regulation and technology tools are the preferred and more effective means than legislation to create trust in electronic business transactions.

The objective of the action plan is to provide an inventory of fundamental business views on the issues that government must deal with and to give a clear overview of business action in those areas where market-driven, industry-led solutions are most likely to be found. The action plan also responds to various high-level statements made by governments in recent years about the need for business to lead the development of electronic business. Business accepts this task and proposes this revised action plan as a mechanism for providing such leadership in a coordinated and transparent fashion.

Part IV of the document presents a sample compilation of successful self-regulatory solutions currently in use or being developed, and indicates progress made in those projects that were also featured in the first and second editions of the Global Action Plan.

Finally, **Part V** describes the Alliance for Global Business.

A previous version of this document was published in 1999 with the title of ‘A Global Action Plan for Electronic Commerce’. It is the intent of the authors for this document to be a “living document” that evolves as electronic business implementation unfolds and provides experience and new evidence of successful projects. To this end, we renew our invitation to readers to submit comments for improvement and, where appropriate, endorsements to:

Ayesha Hassan

Senior Policy Manager, Electronic Business, IT, and Telecoms, ICC

Tel: +33 1 49 53 30 13; Fax: +33 1 49 53 28 59; e-mail: ayesha.hassan@iccwbo.org

2. Fundamental principles

Business believes that a number of fundamental principles should shape the policies that govern electronic business if the promises of electronic business are to be fulfilled. In this context, we provide the following Policy Principles for Global Electronic Business. We expect that these Principles may need to be extended as insights are gained from the development of the marketplace.

1. **The development of electronic business should be led primarily by the private sector in response to market forces.**
2. **Participation in electronic business should be pursued through an open and fair competitive market.**
3. **Government intervention, when required, should promote a stable, international legal environment, allow a fair allocation of scarce resources and protect public interest. Such intervention should be no more than is essential and should be clear, transparent, objective, non-discriminatory, proportional, flexible, and technologically neutral.**
4. **Mechanisms for private sector input and involvement in policy making should be promoted and widely used in all countries and international fora.**
5. **Electronic business is global by nature. Government policies that affect it should be internationally coordinated and compatible, and should facilitate interoperability within an international, voluntary and consensus-based environment for standards setting.**
6. **Transactions conducted using electronic business means should receive neutral tax treatment in comparison to transactions using non-electronic means. Taxation of electronic business should be consistent with established, internationally accepted practices, and administered in the least burdensome manner.**
7. **Regulation of the underlying telecommunications infrastructure, when necessary, should enable actors to compete, globally, in an open and fair market. As competition develops, regulation should be phased out and there should be a greater reliance on competition law.**
8. **The protection of users, in particular with regard to privacy, confidentiality, anonymity and content control should be pursued through policies driven by choice, individual empowerment, industry-led solutions. It will be in accordance with applicable laws.**
9. **Business should make available to consumers and, where appropriate, business users the means to exercise choice with respect to privacy, confidentiality, content control and, under appropriate circumstances, anonymity.**
10. **A high level of trust in the global information infrastructure and services should be pursued by mutual agreement, education, further technological innovations to enhance security and reliability, adoption of adequate dispute resolution mechanisms, and private sector self-regulation.**

3. An action plan

This section aims to provide fundamental business views on:

- (a) the main barriers to the development of electronic business
- (b) solutions already developed by government and business
- (c) the respective roles of governments and business, and, within that context –
 - actions business is taking with respect to specific problems; and
 - actions business considers governments should take.

• **Maximizing the benefits - economic and social impacts**

Electronic business is an innovative approach to ensuring future sustainable economic growth. Throughout the world, the profound impact of electronic commerce on the economies and societies of the globe will undoubtedly improve economic efficiency, competitiveness and profitability and the development of the information society. Within such an environment countries in all stages of development will have the opportunity to benefit by:

- increasing internal organizational and management efficiency;
- increasing transaction efficiency and reducing transaction costs for both suppliers and buyers;
- extending market reach of suppliers and increasing choice for both suppliers and consumers;
- having access to accurate information to improve service delivery such as in health provision, education or the provision of information to consumers.

Electronic business facilitates established business-to-business commercial relations, sales by companies to consumers, and exchanges between consumers. It affects the business environment at national, regional and global levels, and generates major opportunities, and new challenges, for market growth and development of jobs, industries and services. Consequently, internationally coordinated efforts are essential in order to secure the economic benefits of electronic commerce for both the information “rich” and the information “poor”.

Electronic business creates a number of positive impacts, including:

- Shrinking the production and distribution chain by improving intermediation and changing its nature. In addition, using networks to integrate markets directly with suppliers and inventory-tracking procedures can help reduce costs and allow more flexible production methods.
- The ability to compare prices and other terms globally.
- Providing virtual shopping facilities that will change concepts of retailing for a number of goods and services and enhancing the ability of customers to browse and choose new products and services.

- Increasing market competition as costs for consumers are reduced and as market entry barriers for suppliers are lowered, enabling suppliers to address directly market segments that were previously uneconomical.
- Raising productivity growth and the development of new activities will lead to new job creation, but will also result in the demand for new skills.
- Increased employment figures boost government revenues through more taxable income.

Measuring electronic business as accurately as conventional commerce is not easy given the difficulty of defining it and adequately capturing the value associated with it. Nevertheless, such data are needed to focus the policy debate so that action is directed towards activities that accurately reflect electronic commerce and its contributions to economic growth and development.

Small and Medium-Sized Enterprises (SMEs) represent an increasingly important dimension of the global economy. Particular efforts should be made to promote SME involvement in electronic commerce to ensure that they can take maximum advantage of the ability of telecommunications and information technologies to deliver cost efficiencies, quality control and competitiveness in manufacturing and service industries. As one of the most dynamic sectors of a growing economy, SMEs play a critical role in creating employment and enhancing Gross Domestic Product. Electronic commerce provides SMEs with lower market entry costs and the ability to extend geographic reach to a much larger market.

As industry, commerce, and services are transformed by technology, many skills, not only of employees but also of managers and the self-employed, need to be improved or acquired. Future education will include formal and informal learning arrangements and require that it is made available to a much wider range of people, including adults returning to learn. The new information technology, such as interactive media and distance learning, will offer wider access and innovative approaches to education. As future economic prosperity and social and political cohesion depend on a well-educated population, lifelong learning will be essential for everyone as we progress in the 21st century.

It is important to recognize the need for global cooperation by both business and governments to facilitate electronic business. Otherwise, there is a risk that much of the world's population may not be able to participate in the economic and social benefits that can arise from electronic business and information technologies. According to the World Bank, half of the investment needed to upgrade the telecommunications infrastructure in developing and emerging economies will need to come from private capital. Therefore, these countries need to take measures to ensure an appropriate investment climate.

Countries around the world should use electronic means of communications to deliver public services and to make public procurement procedures more efficient. This area requires increased attention to ensure that these processes and services keep pace with best practices. The benefits include government efficiencies, equalization of service provision to all citizens, and the demonstration of government leadership in the use of electronic commerce technology and services.

As the world's richest and most industrialized societies have steadily migrated towards conducting commercial and other activities on the Internet, public policy dilemmas have arisen. The 'digital divide' has become a widely debated policy issue. The term "digital divide" refers to the growing gulf between those who are adequately connected to communications networks and information resources, and possess the means to make best use of these resources, and the two-thirds of the world's population who are not.

So acute is concern, that the leaders of the industrialized world—the Group of Eight or G8—made the digital divide the centerpiece of concern at their 2000 summit meeting in Okinawa. The G8 Digital Opportunity Task Force [DOT Force] was established following that meeting, and it produced a report with concrete recommendations for bridging the international digital divide at the G8 meeting in Genoa, Italy, in July 2001. The DOT Force is marked by close co-operation, on an equal footing, between representatives from G8 governments, developing nations, international organizations, non-profit and private sectors. The DOT Force includes almost 100 stakeholder organizations spanning more than 20 countries. It has generated more than 20 major bilateral and multilateral initiatives. This successful model of co-operation is now serving as the model for other ICT and development initiatives by international organizations and the private sector.

In addition, the United Nations has established the U.N. Information & Communication Technologies Task Force [UN ICT Task Force] which will provide an umbrella for some of the work started by the Dot Force and other international initiatives to build bridges in the digital economy and create the necessary foundations for digital opportunities. The UN and the International Telecommunications Union, in collaboration with other international initiatives, and organizations will host the World Summit on the Information Society in Geneva in 2003 and in Tunis in 2005 and plan to push these initiatives forward and encourage international governmental, private sector and non-profit organizations' cooperation to develop the necessary international environment to overcome the information gap.

Foremost among the findings of the DOT Force and others concerned with the digital divide is a recognition that public communications infrastructure is essential for bridging the unconnected of the world to a rapidly integrating global and largely digital economy. Private sector investment continues to be critical for the construction of needed infrastructure. Governments, international aid agencies, and philanthropic organizations do not have the financial, human, and technical means to construct needed infrastructure. History demonstrates that market-oriented incentives involving the private sector stand the best chance of producing new and sustainable forms of economic activity.

Public policy makers throughout the world increasingly view electronic commerce as more than an otherwise desirable end in itself. It as a powerful economic dynamic which, if allowed to flourish and evolve as quickly and effectively as possible, will foster and speed the deployment of public communications infrastructure, and begin to close the gap between the world's information "have's" and "have-nots".

	Business action / observations	Government action required
1. Economic and social impacts	Business organizations will continue to support studies and analyses of the impact of electronic commerce and share these finding with governments and international organizations.	<p>Governments are encouraged to inform both individual consumers and businesses, about the potentials of electronic business and its impact on social and economic structures.</p> <p>Governments and international organizations, notably the OECD, should be encouraged to continue to collect and analyze data relevant to the study of electronic commerce in order to effectively measure its economic and social impact.</p> <p>International development organizations such as the World Bank should continue to study the potential impact of electronic commerce on emerging economies in an effort to assist in the economic development process in those nations.</p>
2. Small and medium sized enterprises	Business organizations and chambers of commerce will promote marketing and technology support for SMEs through information brochures, collection and communication of sector-specific best practices and workshops. Business will encourage greater interaction between large corporations and SMEs to provide access to electronic business networks for supplier and contracting opportunities.	<p>Government should provide SMEs with information and education relevant to market entry opportunities provided by global electronic commerce.</p> <p>Governments should create an environment that is conducive to private sector investment in information technologies and encourage capital access for SMEs.</p>

	Business action / observations	Government action required
3. Skills development	Business is committed to continue to work with government to promote technical training and life-long learning for all in society.	<p>Governments should review existing labour laws to remove existing barriers for workers to be able to share in the new and different employment generated by electronic business.</p> <p>Governments should continue to promote both formal and non-formal skills-development programs.</p>
4. Ensuring global participation / Seizing Digital Opportunities	<p>Existing business organizations will work to expand the participation from business in developing countries in promoting the uses and benefits of electronic business.</p> <p>Business will expand its advisory role with international organizations dealing with electronic business issues.</p>	<p>Existing international organizations should increase cooperation, as well as coordination and transparency of their respective work programmes.</p> <p>All governments should use a policy framework that ensures open and competitive markets for electronic business as a means of maximizing access to digital information and communication networks for all. A liberalized trade regime for services, IT goods and timely and effective implementation of TRIPS (Trade Related Intellectual Property Issues) is an essential element to such a framework, providing opportunities for developing countries to leapfrog technologies and services that have required enormous research and development.</p>

	Business action / observations	Government action required
5. Infrastructure deployment	Business will remain an important driver in the development of the information infrastructure because it mobilizes the private capital needed to build the global information infrastructure and to develop the technological innovations that enhance communications.	<p>As telecommunications continues to transition from a monopoly to competitive environment, a crucial role for the government is that of being a neutral force in the economy that ensures pro-competitive behaviour, transparent rules, and value to the customer.</p> <p>International organizations should provide a forum for coordinated government action and international cooperation on matters relating to global development. Agreements drawn up by multilateral organizations offer the private sector and governments the necessary legal and regulatory certainty for investment.</p>
6. Government as model user	Business will work with governments to offer cost-effective electronic delivery systems for the public sector.	<p>Governments are encouraged to use new electronic delivery systems to provide the means to significantly enhance the internal efficiency and productivity of public administrations. Governments should be pioneers in using new technologies for making electronic forms available for collecting taxes and other functions.</p> <p>Governments should promote electronic business through its public procurement system, done in a fully open and competitive environment, based on cost-efficient, commercial solutions that are technology neutral.</p> <p>Governments are also encouraged to use new electronic means to deliver core public services. In particular this would concern public information and cultural resources, databases for health services, web sites at local, regional and national levels and public libraries and databases, where appropriate.</p>

Electronic business and the information infrastructure – trade aspects, standards, and Internet names and numbers

Competition and trade-related aspects of electronic business

On September 25 1998, the WTO Declaration on Global Electronic Commerce began "a comprehensive work program to examine all trade-related issues relating to global electronic commerce, taking into account the economic, financial, and development needs of developing countries...". Four WTO bodies -- The Committee on Trade and Development, The Council on Trade-Related Intellectual Property, the Council on Goods, and the Council on Services -- reviewed how existing multilateral trade agreements apply to global electronic commerce.

The 2001 WTO Doha Ministerial Declaration's section on electronic commerce said " We take note of the work which has been done in the General Council and other relevant bodies since the Ministerial Declaration of 20 May 1998 and agree to continue the Work Programme on Electronic Commerce. The work to date demonstrates that electronic commerce creates new challenges and opportunities for trade for countries at all stages of development, and we recognize the importance of creating and maintaining an environment which is favourable to the future development of electronic commerce. We instruct the General Council to consider the most appropriate institutional arrangements for handling the Work Programme, and to report on further progress to the Fifth Session of the Ministerial Conference..."

Open competition in the provision of products and services at all levels of the information society is a prerequisite for the development of electronic business. Regulation of the underlying telecommunications infrastructure, when necessary, should enable actors to compete globally in an open and fair market. As competition develops and is relied upon more, regulation should be phased out. The convergence of telecommunications, IT and multimedia raises important questions that require international attention for liberalization efforts to produce optimum results.

	Business action / observations	Government action required
4. Telecommunications competition	<p>Business remains committed to providing practical information about appropriate competitive safeguards. Business will continue to call on governments to set and implement conditions for open and fair competition.</p> <p>Business is studying means of avoiding and settling commercial disputes between competitors to provide an alternative to resolution by regulatory agencies.</p>	<p>Effective implementation of the WTO agreement on basic telecommunications is of critical importance. In consultation with business, governments with experience in telecommunications liberalization should actively assist signatory countries that still have to start this process. Countries that have scheduled commitments under the WTO agreement on basic telecommunications should review the extent to which their markets are fulfilling the agreement, publish their findings on a regular basis and work towards the elimination of MFN exemptions.</p>

**Telecommunications
competition (continued)**

The OECD, ITU and WTO – within their respective domains - have a role to play in facilitating such assistance.

Efforts to promote full implementation of existing commitments and seek increased liberalization for all basic telecommunications, value-added and computer and related services need to continue following the new round of negotiations launched in Doha in November 2001.

Business urges WTO members to include as one of the highest WTO negotiating priorities in any accession protocol market opening commitments in basic telecom services that at a minimum include: (1) specifying a date certain for full liberalization, (2) progressively removing foreign ownership restrictions and (3) adopting the reference paper in its entirety.

**Business action /
observations**

Government action required

5. IT equipment

Business has been a staunch supporter of the ITA and its extension to more participants and products. It is desirable that IT products are integrated into mainstream WTO market access negotiations in the context of the Doha negotiating mandate.

Governments should ensure that all countries have the hardware and software necessary to deploy and access the e-business infrastructure by eliminating duties on all IT products to fully realize the objectives of the Information Technology Agreement, including commitments at the broadest level for categories 84, 85, and 90.

To that end, governments should commit to including these products in the upcoming market access negotiation on non-agricultural products in the course of the new round of negotiations launched at Doha.

	Business action / observations	Government action required
6. Trade-related aspects of electronic commerce	In response to the WTO's work programme to examine all trade-related issues relating to global electronic commerce, business has responded in a constructive way by issuing papers on the trade-related aspects of electronic commerce.	<p>WTO members should recognize that specific WTO agreements governing trade in goods, trade in services, or trade-related intellectual property apply to electronic transmissions. WTO members should continue to address the issue of classification of electronic transmissions as either goods or services in their ongoing work programme ensuring trade treatment and classification of electronic transmissions that is as similar as possible to and no less favorable than the historical treatment applied to the underlying good, service or intellectual property.</p> <p>Electronic transmissions are blind with regards to national borders. Thus, WTO members should agree to make permanent duty free treatment of electronic transmissions.</p> <p>Continued development of electronic business requires the ability to conduct cross-border transactions. Negotiations following the WTO Doha Ministerial Conference negotiations should promote the adoption of meaningful market opening commitments in all service sectors, especially for all services that can be delivered via e-commerce.</p> <p>With the rapid development of digital technologies and electronic services, the need for strong protection and enforcement of intellectual property is imperative. The TRIPS Agreement plays a very important role insofar as it provides minimum standards for such protection and enforcement.</p>

	Business action / observations	Government action required
7.	Trade-related aspects of intellectual property	<p>Business will work to encourage all countries to implement effectively the TRIPS agreement. Business will also continue to develop and deploy technologies that prevent IP infringements in the online environment.</p>
8.	Convergence	<p>Businesses are already developing, providing and using products and services taking full advantage of the convergence phenomenon. These developments are likely to accelerate.</p> <p>Convergence of technologies is leading to the need for concomitant convergence in regulation of broadcasting, IT and telecoms. Convergence is crucial to electronic business and must be supported by appropriate government policies. Governments should work closely with business in preparing for and reacting to changes caused by convergence by applying the following principles:</p> <ul style="list-style-type: none"> • Competition policy should be used as much as possible as the predominant means of preventing abuses of market power in the telecommunications and media sectors. • Government regulation should be limited to promoting fair competition, allocating scarce resources and protect the public interest. • Governments should recognize that technological neutrality is a concept to promote competition, not to extend existing regulation to new activities.

Standards

Electronic business offers great economic efficiencies, linking all parts of a transaction into one integrated end-to-end chain. Government policies should facilitate interoperability within an international, voluntary and consensus-based environment for standards setting. The market needs a fully interoperable architecture, which is being developed within existing standards-setting institutions or by market forces. In addition to enforcing appropriate competition laws, governments should ensure that standards are accepted by customs, taxation and other relevant governmental agencies. Government should refrain from developing competing standards through procurement mechanisms. Where market mechanisms do not respond to government procurement needs, the private sector and government should work together to develop a responsive, inter-operative interface.

	Business action / observations	Government action required
Standards	<p>There are numerous efforts to develop standards relating to electronic commerce, including privacy, electronic signatures, etc.</p> <p>Standards for electronic business should continue to be market driven and industry-led.</p> <p>Business will continue to work with all relevant international standards-making bodies to develop international standards that provide added value and are necessary for the development of electronic business.</p>	<p>Governments should avoid mandating unnecessary technical standards that could be or are being led by business.</p>

Internet names and numbers

Because the Internet is rapidly becoming the vehicle for global electronic commerce, the management of the domain names system is of great importance.

	Business action / observations	Government action required
1. Domain name system	Business should have a significant role in the formation of policy for technical management of the domain name system and the development of policy. Through the various Supporting Organizations of the Internet Corporation for Assigned Names and Numbers (ICANN), and in particular the Business Constituency of the Domain Name Supporting Organization (DNSO), business will continue to work to ensure continued stability and security of the Internet, as well as appropriate protection of intellectual property. The protection of intellectual property (especially famous names) and efficient ways of dealing with cybersquatting remain priority issues for business.	Governments should <ul style="list-style-type: none">• continue to support ICANN and its private sector leadership;• support initiatives to ensure that the business community will have a sufficient voice in the technical management of the domain name system.

Building trust for users and consumers

The protection of users, in particular with regard to privacy, confidentiality, anonymity and content control should be pursued through policies driven by choice, individual empowerment, industry-led solutions, and will be in accordance with applicable laws.

Business will make available to users the means to exercise choice with respect to privacy, confidentiality and content control.

Protection of Personal Information

	Business action / observations	Government action required
1. Privacy and transborder flows of data	<p>Business endorses the OECD 1980 Guidelines for the protection of Privacy and Transborder Flows of Personal Data, and is committed to implementing fair information practices and transparent procedures consistent with these Guidelines.</p> <p>Business uses model contracts and internal control procedures to satisfy requirements of legislation restricting export of data to third countries that do not provide a level of protection considered to be adequate or sufficient by the source country. The use of model contracts provides a flexible, market-based solution for meeting differing data protection standards in the conduct of global business.</p>	<p>Governments should 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.</p> <p>Provided the principles in the OECD Guidelines are met, different approaches to the protection of personal information should not prevent transborder data flows, and governments should cooperate internationally to ensure a seamless environment. 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 honoured within that jurisdiction.</p> <p>Model contracts and codes of conduct prepared by the private sector should be endorsed by relevant governments at the earliest possible time to promote the free and secure flow of information.</p>

	Business action / observations	Government action required
2. Internet privacy	<p>Business is committed to work with governments to ensure non-discrimination among culturally different but adequate regimes for protection of personal information in the digital environment</p> <p>Business is developing, based on global marketplace experience, fair information practices that are consistent with the OECD 1980 Guidelines for the Protection of Privacy and Transborder Flows of Personal Data. It does so through self-regulation, voluntary codes and by making commercially available technologies enabling a high level of privacy protection tailored to user needs and preferences.</p> <p>The use of third-party compliance schemes is growing rapidly in response to market forces. The rate with which such schemes are being adopted in some jurisdictions demonstrates a strong commitment by the private sector to embrace consumer satisfaction as a competitive issue. Effective self-assessment programs have been and continue to be implemented by the private sector.</p> <p>Business is continually reviewing existing self-regulation to ensure that it takes into account new technologies and provide effective and credible privacy protection.</p>	<p>Governments should recognize that the Internet is a new medium providing new opportunities and challenges. Existing regulatory systems must provide consumers with useful protection of their personal data and at the same time guarantee the free flow of information needed for the information society to produce the anticipated benefits. Governments should also recognize that self-regulation may be a more flexible method of achieving data protection than government regulation.</p> <p>To that end, governments should:</p> <ul style="list-style-type: none"> • work with the private sector to adopt interpretation of existing regulatory solutions based on the criteria in the paragraph above; • recognize the validity and adequacy of effective self-regulation augmented by the use of privacy-enhancing technologies; and • educate the public to use such privacy-enhancing technologies properly. <p>Any privacy measures taken by governments should not be more restrictive than necessary or be applied in a manner which is a disguised restriction on trade in services as set forth in Article XIV of the GATS. Current international initiatives to enhance privacy protection on a global basis should be taken into consideration when assessing the need for such measures. They also must not constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade in services.</p>

Consumer trust and content

Within a freely functioning global electronic marketplace, increasingly sophisticated user-friendly tools and business practices for empowerment of consumers have been and continue to be developed and implemented. Retail websites offering wide ranges of consumer choice and providing individualization of the consumer experience are succeeding in gaining customer support.

By its very nature, online business-to-consumer (B2C) commerce is exponentially more cross-border in nature, thus potentially subjecting merchant and consumer to problems of jurisdiction and applicable law whenever a dispute arises. Effective dispute resolution is an essential element of consumer trust. The private sector is developing and implementing effective self-regulatory mechanisms and governments are contemplating legislative steps to reduce the risk of conflict. Governments, business and consumers alike agree that effective alternative dispute resolution is an efficient and cost-effective means of resolving consumer disputes.

	Business action / observations	Government action required
1. Consumer trust	<p>Increasingly sophisticated empowerment tools for consumers continue to be developed and implemented to protect and empower consumers in a truly global marketplace.</p> <p>Consumer protection is an essential element of building trust in the online environment and is directly complementary to market principles of consumer service and satisfaction. Companies that safeguard consumer interests stand to gain a business advantage.</p> <p>Business is developing and deploying policies and mechanisms that provide informed consumer choice.</p> <p>Business is taking the lead in developing user friendly dispute resolution mechanisms as a means of resolving consumer disputes in a rapid, efficient and cost-effective way.</p>	<p>Consumer protection should develop from appropriate business/consumer platforms. Business, and interested parties, should be fully involved in international discussions to set policies for consumer protection.</p> <p>Governments have a major role in educating and empowering the public to enhance awareness of their responsibilities and ability to exercise choice with respect to their protection as consumers.</p> <p>Governments should adopt "opt-out" procedures as the most appropriate balance between consumer trust and choice with regard to unsolicited commercial communications, cookies, directories, etc. Any other approach would discriminate against electronic business vis-à-vis other communications mechanisms.</p> <p>Governments should promote a systematic approach to the resolution of consumer disputes, encouraging consumers to;</p> <ul style="list-style-type: none"> • make reasonable attempts to utilize a company's internal customer satisfaction mechanisms; • utilize online alternative dispute resolution (ADR); and • if the dispute persists, resort to legal action.

	Business action / observations	Government action required
2. Online Alternative Dispute Resolution (ADR)	<p>Business and other organizations should continue to develop and implement effective B2C ADR systems which meet certain minimum standards concerning, for example, accessibility, attentiveness, global flexibility, compliance, and the nature of decision. Moreover, they should have in place workable internal complaint systems which also meet certain minimum standards, in order to reduce the chance of disputes requiring B2C ADR. Internal complaint-handling systems should be timely and transparent to ease any eventual outsourcing of a dispute to B2C ADR should the complaint not be resolved internally.</p> <p>ICC in cooperation with the OECD has completed a comprehensive inventory of online and offline dispute resolution service providers that handle B2C and C2C disputes arising out of online transactions.</p>	<p>Governments should refrain from imposing mandatory national or regional accreditation systems. Rather, they should promote the development of international self-regulatory principles, guidelines and rules that could be the basis for merchants' and B2C ADR providers' declarations of compliance.</p> <p>Governments should promote the development of globally applicable B2C ADR systems.</p> <p>Governments should refrain from creating obstacles in national legislation and international conventions for the innovative use of technology, including electronic contracts, to settle business-to-consumer disputes and eliminate legal obstacles to allow an appropriate level of confidentiality and security in online B2C ADR. Such legal obstacles include unnecessary legal form requirements that hinder the use of online B2C ADR, and the requirement for B2C ADR to meet all the same procedural requirements as litigation in court.</p> <p>Governments should provide a legislative framework for jurisdiction and applicable law in e-commerce which recognizes the importance of B2C ADR systems for business-to-consumer transactions.</p>

	Business action / observations	Government action required
3. Content	<p>Technological developments have had and will continue to have a profound impact on culture. However, the emerging digital environment can provide ample distribution capacity for all content, alleviating "competition" among different types of content. In addition, the interactivity of the new technologies enables users to choose among different types of content and governments should not interfere in this personal decision-making process.</p> <p>Business continues to develop and implement voluntary content rating and filtering technologies to empower consumers.</p>	<p>Content regulations are based on different legal and cultural traditions. Nevertheless, content regulations should be kept to a minimum as they restrict the free flow of information into the marketplace of ideas. Where content regulations exist, it is the role of the appropriate law enforcement authority to enforce the law. In the context of potentially inappropriate, but otherwise legal content, business encourages the use of market-driven solutions, including the numerous filtering and blocking technologies rather than restricting access to such content through regulation. Such technologies empower the consumer to make informed decisions about the type of content he/she wants and does not want to access.</p> <p>Governments should enforce existing laws relating to illegal content.</p> <p>Any legislation that deals with the issue of liability should carefully consider the effect such laws have on the interests of all stakeholders in the electronic environment, and, where clarifying liability rules for intermediaries, needs to strike a careful balance between the legitimate business interests of the different stakeholders involved, including content providers, service providers and end-users.</p>

	Business action / observations	Government action required
4. Marketing and advertising ethics	<p>Business in many countries has a mature system of self-regulatory complaint mechanisms and cooperative enforceable self-regulation for advertising practices, such as industry or trade associations, chambers of commerce, and better business bureaus.</p> <p>The concept of business self-regulation of marketing ethics continues to evolve to adapt to the online environment through international cooperation and agreement.</p> <p>As a complement to existing legal instruments, self-regulatory guidelines and voluntary industry norms, such as those developed by the International Chamber of Commerce, also play an important role in promoting high standards of consumer protection.</p> <p>Business will continue to improve upon self-regulatory solutions for Internet advertising and market research. Business is establishing appropriate international self-regulatory enforcement mechanisms for violations of such best practice rules.</p>	<p>In the borderless global environment of the Internet, internationally incompatible national laws on advertising and promotions seriously impede cross border sales.</p> <p>Governments should support self-regulation for Internet advertising at the global level based on the existing good cooperation between government agencies and business self-regulatory bodies for traditional advertising at the national level.</p>

	Business action / observations	Government action required
5. Unsolicited Commercial Communications	Business is attempting to eliminate fraudulent and untargeted commercial communications (spam) and is working to provide choice relating to legitimate commercial email.	Governments should distinguish between fraudulent and untargeted commercial communications (spam) and commercial email, prohibiting spam while recognizing that commercial email can play a legitimate and significant role in the emergence and growth of electronic commerce. To that end, an "opt-out" approach should be adopted as the most effective means of balancing consumer trust and choice for legitimate commercial email.

Issues relating to cyber security

Cyber security is essential in promoting trust for both business and consumers. Three general activities relating to cyber security are currently part of the public policy debate:

1. Protecting critical information infrastructures to ensure national security and the security of society at large;
2. Ensuring public safety through law enforcement and fighting cybercrime; and
3. Promoting economic security.

Governments directly, and through regional bodies such as the EU, NAFTA, FTAA and APEC, have roles to play in the two first areas by securing their own national and regional networks as part of their critical infrastructure responsibilities, and agreeing on a comprehensive international law enforcement platform with the private sector and other stakeholders. Economic security is largely the domain of the private sector, though a dialogue with government is essential to build consistency with the first two activities.

The steps that need to be taken to address these three activities include:

- ensuring the confidentiality of personal and business information;
- establishing mechanisms and procedures to prevent security breaches and sufficient disaster control plans;
- adopting laws necessary to establish malicious acts as criminal; and
- developing appropriate mechanisms for co-operation between business and law enforcement.

The business community recognizes the efforts made by governments on issues relating to cyber-security. The Wassenaar Arrangement has liberalized its export restrictions on mass market encryption products and other states have liberalized their cryptography policies. The OECD is undertaking a review of its Information Security Guidelines. The Council of Europe has ratified a convention on cybercrime which signatory states are beginning to implement, and the G8 has been working on cybercrime and national security issues. Business looks forward to continuing to working with governments on these initiatives.

	Business action / observations	Government action required
1. Promotion of technology and services development to ensure security	Business continues to develop and deploy technology and services for ensuring security in order to build trust in electronic commerce.	Governments should support private sector leadership in the development and deployment of technology solutions and services and fundamental private sector research and development relating to security technology.

	Business action / observations	Government action required
2. Cryptography for confidentiality	<p>It is crucial for electronic commerce that business and end-users are able to choose the cryptographic systems that best suit their needs, and that these systems can function internationally. To that end, business applauds the efforts of numerous governments to liberalize their cryptography policy.</p> <p>Business is opposed to any mandatory system based on a specific technology. Business will continue to develop and implement cryptographic products allowing a high level of confidentiality. Business is prepared to continue to discuss possibilities to protect law enforcement and national security.</p>	<p>The OECD cryptography policy guidelines were an important step in the direction of a uniform international approach. The urgent need for strong encryption in electronic commerce necessitates the next step in this co-operation between business and government. Governments must allow electronic commerce to thrive in a free market by continuing to remove obstacles to the use of publicly offered encryption solutions.</p> <p>Governments should commit to:</p> <ul style="list-style-type: none"> • remove all controls on cryptographic technologies and applications; and • cooperate in such a way that interoperability of solutions for internationally secure exchange of information is facilitated, independent of their choice of regulation.
3. Information Sharing	<p>Information sharing is an essential element in enhancing security, including prevention of security breaches. In that regard, business is working with governments through Information Sharing and Analysis Centers (ISACs) which have been created in the U.S. and are being established in other countries. Moreover, business has created information sharing and analysis websites, listserves, email alerts and other services to promote information sharing.</p>	<p>Governments should support the development of ISACs and should recognize private sector leadership in protecting the information infrastructure.</p>

	Business action / observations	Government action required
4. Cybercrime	<p>Business is committed to cooperating with law enforcement in a manner consistent with business realities and therefore welcomes the current discussions between governments and industry regarding cybercrime and security. 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.</p>	<p>Governments should ensure that the appropriate legislation and resources are in place to investigate and prosecute cyber attacks.</p> <p>Business recognizes the improvements in the Council of Europe Convention on Cybercrime. As signatories begin to implement the Convention they should contemplate:</p> <ul style="list-style-type: none"> • preventing conflicting privacy and security obligations; • limiting service provider liability in a manner that balances the interest of all interested parties including copyright owners, service providers and users • adopting clear procedural safeguards; • providing for reimbursement for costs of compliance; • identifying the appropriate circumstances for corporate liability; • maintaining criminalization of copyright infringements; • ensuring consistency between the “misuse of devices provisions of the Convention and existing law concerning “anti-circumvention”.

	Business action / observations	Government action required
5.	<p>Business monitoring of its own communications and networks</p> <p>Businesses need to be able to monitor communications over their own networks to verify and/or prove business transactions and for quality control or training purposes for the benefit of the customer. Some regulatory initiatives restrict these legitimate practices.</p> <p>Businesses need to be able to monitor traffic flow over their own networks to ensure that it conforms to expectations thereby identifying potential security attacks.</p>	<p>Governments should ensure that businesses are entitled to monitor communications over their own networks for legitimate purposes such as the improvement of customer service, the verification or proof of a business transaction, quality control and training, with the consent of only one party to the communication.</p> <p>Governments should ensure that businesses are entitled to monitor network traffic flow over their own networks as a means of enhancing efficiency and network security.</p>
6.	<p>Data Storage Requirements</p> <p>Business fully supports appropriate cooperation with law enforcement to enhance security, being mindful of business realities.</p>	<p>Governments require data for law enforcement purposes. Businesses should be required to preserve data in their possession only upon receipt of a subpoena (or written functional equivalent thereof) issued by a competent judicial or administrative authority that follows appropriate due process, is narrowly tailored to meet the needs of a specific investigation or prosecution, is limited in duration, and is conducted in an expedited way.</p>

	Business action / observations	Government action required
7. Searches and subpoenas of computer records	Business recognizes the need for lawful access to computer records and co-operates with law enforcement as appropriate. However, there is an urgent need to ensure that law enforcement practices and policies reflect a clear understanding of how computers work, how businesses use them, and the extent to which traditional approaches to the collection of computer records may unnecessarily impose significant costs on business.	When requesting, issuing or executing a search warrant or a subpoena, government law enforcement agencies should take due care to cause the least burden to the operations of the subject firm, to respect privacy and confidentiality requirements, and not to overstep the territorial scope of the subpoena or search warrant by exploiting computer linkages with sources in other locations. Law enforcement agencies should not use the firm's computers to access or seize information stored on computers outside their jurisdiction but rather rely on existing procedures such as mutual legal assistance treaties and legislation.
8. Access to public domain information	To ensure that the information business holds is correct and to promote efficiency and consumer satisfaction, business needs access to public domain information to conduct its transactions. Business will develop international principles, as appropriate, to guarantee commercial use of personal information, prevent liability for the use of public data, and promote the availability of such data for legitimate commercial purposes.	Governments should guarantee equal and transparent access to public domain information to ensure business' legitimate interests, whilst recognizing the need to achieve a balance with the protection of personal information.
9. Legal government interception of telecommunications and electronic communications	The development of acceptable international standards is important. Business is concerned that the wide range of government organizations devising standards may lead to inconsistencies.	Discussions that may affect existing wiretapping safeguards should include business participation as a matter of principle.

Electronic authentication

Electronic signatures^{*}, are important to ensure proper identification of communicating partners, and authenticity and non-repudiation of messages that they exchange. For this to be realized, a number of international actions need to be taken. 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. Many countries are developing, or have already implemented, electronic signature laws that include rules pertaining to certification services. Governments have an important role to play in assuring the legal validity of electronic signatures.

	Business action / observations	Government action required
1. Legal validity of electronic signatures; interoperability of certificates and electronic signatures	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 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.”

	Business action / observations	Government action required
Legal validity of electronic signatures; interoperability of certificates and electronic signatures (continued)	<p>Business supports freedom of contract to establish parties' rights and responsibilities when using electronic signatures. Contracts enable parties to agree on the acceptance of electronically signed data and on the terms and conditions of transactions (including limitations on liability). Contracts can also include the following: methodologies for enforcing online contracts and resolving disputes; compelling public policy considerations such as public safety and prevention of fraud issues; and use of appropriate terms and conditions.</p> <p>Business looks forward to working with governments within relevant bodies in this field.</p> <p>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.</p>	<p>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; and promote competition among providers of authentication services.</p> <p>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. Neutral criteria relating to adequacy should be used to determine recognition.</p> <p>Standards for electronic signatures that are used or recognized by governments should be technology neutral, commercially available, not endorse or favour any particular solution and should allow for technological innovation.</p>

	Business action / observations	Government action required
2. Accreditation	<p>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. As electronic business is an emerging market, the marketplace may require different kinds or levels of accreditation or certification. Accreditation or certification may not be required in every instance. Those that undertake the accreditation or certification of certificate authorities should be held liable for their certification actions. Therefore any accreditation solution should be developed in response to a specific market need and tailored to address a well-defined requirement.</p>	<p>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.</p>
3. Availability of certification practice statements	<p>Business is developing best practices for providing adequate notice to consumers of the responsibilities of Certification Authorities. Business is developing innovative services and technologies to provide easy access to notices of these responsibilities.</p>	<p>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. If required, accreditation should be voluntary, based on internationally recognized best practices.</p>

Establishing ground rules for the digital marketplace

Contractual and other legal issues

Freedom of contract must prevail as the underlying principle of all efforts to create an appropriate legal environment for business-to-business transactions. Governments can support electronic commerce by enabling electronic contracting and by facilitating the legal recognition of digitally authenticated documents and contracts. Governments should avoid prescriptive and detailed legislation in these areas and ensure the development of facilitating legislation, which may assist the private sector in developing self-regulatory solutions.

	Business action / observations	Government action required
1. Removing legal/regulatory obstacles	<p>Traditional self-regulatory solutions for international trade are continually being adapted to new business practice.</p> <p>The global business community is analyzing existing legal and policy barriers to the digital marketplace, and will make recommendations where appropriate.</p> <p>Business is developing technologies and procedures that enable the creation and determination of electronic "originals".</p>	<p>Countries should implement the UNCITRAL Model Law on Electronic Commerce, which provides for a particular country to address issues specific to its jurisdiction, as soon as possible.</p> <p>UNCITRAL is currently considering work on removing barriers to electronic contracting. Some international conventions need to be adapted (UN-ECE has published an analysis of international work to be done). The good cooperation that exists among private and public sector international legal expert bodies should be a model for future cooperation between business and governments with respect to electronic business.</p>

	Business action / observations	Government action required
2.	<p>Create a new uniform legal framework</p> <p>Through various private-sector trade promotion and facilitation organizations, a framework of self-regulatory rules for electronic business is evolving. In general, market forces should lead but business acknowledges that for some key issues there is no self-regulatory substitute for a reliable legal framework to provide certainty and confidence in electronic business.</p>	<p>Governments should continue to work at the international level to create a coherent legal framework to enable electronic business.</p>
3.	<p>Jurisdiction and applicable law</p> <p>Business will work with governments to find solutions to the problems associated with determining jurisdiction and applicable law in cyberspace. Alternative dispute resolution mechanisms and third-party schemes for compliance with self-regulation are being developed by existing and new types of providers of dispute avoidance and resolution.</p>	<p>Freedom of contract should be the guiding principle for business-to-business (B2B) and business-to-consumer (B2C) relationships.</p> <p>Governments should avoid expansive claims of jurisdiction in the B2B context by applying principles of country of origin and party autonomy and allowing self-regulation to demonstrate its efficacy.</p> <p>The Hague Conference is currently negotiating a Convention on Jurisdiction and the Enforcement of Foreign Judgements in Civil and Commercial Matters. Given the jurisdictional complexities raised by electronic commerce and the lack of consensus among stakeholders on many jurisdictional issues, governments should limit the scope of the convention to business-to-business contractual activities with strong party autonomy.</p> <p>Governments should rely on voluntary business self-regulatory practices and market pressures to develop more flexible and balanced solutions.</p> <p>The use of alternative dispute resolution for consumers should be encouraged while maintaining court proceedings as the ultimate solution in case of unresolvable conflicts.</p>

	Business action / observations	Government action required
4.	Incorporation by reference	In electronic business, terms of legal significance will increasingly be incorporated into contracts by reference. Business will continue to develop more effective, transparent and user-friendly delivery mechanisms for the full definitions of such terms.
		Governments should continue work on basic international principles for legal validity of incorporation by reference for all kinds of transactions. These rules should aim to provide certainty for all parties to electronic business transactions.
5.	Transparency & availability of proprietary & best practice legal terms, model contracts, etc.	Online legal databases with user-friendly reference systems are being made available for use by parties conducting online transactions.
		Governments are encouraged to promote such business-driven repositories and to contribute public legal terms and instruments to them.
6.	Dispute settlement	Speed and expertise in settling electronic business disputes are important. Providers of alternate dispute settlement systems are implementing and continue to test tailor-made voluntary systems appropriate for the settlement of online disputes.
		Governments should encourage the use of self-regulatory dispute settlement mechanisms as an effective way of resolving electronic business disputes. Courts should urgently develop electronic business expertise.
7.	Fraud and other commercial crime	Business will continue to advise governments on appropriate action to combat electronic business fraud. Specialized business organizations will continue to provide information on fraud and fraudsters to the business community and, where appropriate and under adequate confidentiality arrangements, to law enforcement.
		Criminal laws, courts and enforcement agencies should develop more expertise to deal with electronic business fraud and computer crime. When applying national criminal laws, government should take into consideration the global nature of electronic business. Close cooperation among governments and between governments and business is vital in this process.
		Electronic authentication techniques are important for users to protect themselves against fraud. Their legal validity should be addressed as soon as possible.

	Business action / observations	Government action required
8. Liability	Business will review general questions of liability in electronic business and submit its findings to relevant governmental organizations.	Freedom of contract should be the guiding principle. Governments should avoid creating liability rules that can impede the advancement of electronic business and should work with business to identify areas where liability rules are required.

Taxation and tariffs

Tax and tariff policy will be instrumental in determining whether the vast potential of global electronic business can be realized. The development of electronic business is a change in the way in which international business is conducted and requires a fundamental review of tax policies and laws, which have their origins in traditional, off-line commerce. Fundamentally, however, electronic business should compete with traditional commerce on a level playing field. Tax systems should not interfere with the operation of a market economy. A global perspective is required when addressing this subject, as electronic commerce cuts across national boundaries to a greater degree than traditional forms of business. Therefore, consistent taxation approaches at the international level are absolutely critical to ensure the effectiveness of tax treatment in the digital economy and the avoidance of double taxation.

Similar income should be treated equally in terms of direct and indirect tax requirements, regardless of whether it is earned through electronic means or through traditional channels of commerce. Electronic business however should not be the target of new and discriminatory taxes. The application of existing taxation on electronic commerce should be governed by the principles of tax neutrality and fairness.

Many taxation issues are not new or unique to electronic commerce but have already developed in conventional business transactions, which increasingly relies on new modes of communications and increasingly crosses national borders. The mode of doing business through electronic means may add new layers of difficulty but does not create a new problem. Any legal obligations should not be restricted to electronic business but should apply equally to conventional business as well.

The request for a tariff-free zone for electronic transmissions is based on a long tradition of reducing or eliminating barriers (such as customs duties) to international trade. Lowering trade barriers, including tariffs, is one of the most obvious means of encouraging international trade as well as global electronic business.

	Business action / observations	Government action required
1. Customs duties	<p>Business is working with governments to ensure that the international trading system is as free as possible from barriers to trade, including custom duties.</p> <p>Commitments in this area make the business environment stable and predictable and give business a clearer view of their future trade opportunities. With stability and predictability as part of the multilateral trading system, trade increases, investment is encouraged, jobs are created, and consumers can enjoy the benefits of competition -- choice and lower prices.</p>	<p>The WTO May 1998 Moratorium on Customs Duties on Electronic Transmissions recognizes that cross-border electronic transmissions are not now considered imports subject to customs duties or border controls. There are no customs duties or border controls on telephone calls across borders; there are no customs duties or border controls on fax messages; and, there are no customs duties or border controls on email or computer links.</p> <p>At the 2001 WTO Doha Ministerial Conference, members agreed to maintain their current practice of not imposing customs duties on electronic transmissions until the next Fifth WTO Session. For stability and predictability in international trade in the 21st Century, WTO members should make permanent the duty-free treatment of electronic transmissions and should consider in their ongoing work programme on electronic commerce to move beyond a temporary commitment to a permanent one.</p>

	Business action / observations	Government action required
2. Taxation	<p>Business strongly supports the use of partnership working groups between business and government – such as the OECD Technical Advisory Groups - to address the numerous taxation issues relating to electronic business.</p> <p>Business is working with tax authorities to open this process broadly to interested business participants. We believe that to ensure the widespread support of the business community, even greater openness is called for to ensure timely and valuable input by those in the business community who have much to offer this process.</p> <p>We also heartily endorse efforts to seek a truly international consensus on these taxation issues</p>	<p>Governments should work with industry in international fora such as the OECD Technical Advisory Groups. There should be no additional taxes, such as usage or bit taxes. Future taxation policy on electronic business should:</p> <ul style="list-style-type: none"> • be consistent with the principles of international taxation; • be neutral with regard to other forms of commerce; • be consistent across tax jurisdictions; • avoid double taxation; • minimize compliance costs; and • be transparent, predictable and with simple rules to follow. <p>Applying existing taxation principles in the electronic medium must also be built upon tools that businesses already use or are required to develop to meet their market needs - it is only in this way that high tax compliance can be sustained with the least burden, and the fewest economic distortions.</p>

Trade facilitation and customs modernization

For business to use fully the benefits of electronic commerce, documentation in electronic form should not be denied legal acceptability solely on the grounds that it is in digital form. The handling of customs documentation, for example, will be both faster and more cost effective if it can be made in electronic form. The legal acceptability of auditing records and receipts in electronic form from electronic business transactions are other examples of modernization that can substantially reduce costs and facilitate and promote electronic trade.

	Business action / observations	Government action required
1. Private/public sector interface	Business and governments should work together to ensure compatibility between standards at appropriate interfaces.	Work on customs data requirements is under way in the WCO and the G7. In other fields, there does not seem to be an organized effort to harmonize requirements. OECD would be an appropriate forum to address interface issues relating to taxation.
2. Customs modernization	Business is keen to continue to cooperate with governments within the World Customs Organization (WCO) and WTO on issues relating to customs modernization. Business will also continue to work with and advise customs authorities on issues relating to electronic business.	<p>To enable businesses and consumers to reap the benefits of electronic commerce, governments should work through the WCO and WTO to enhance the efficiency and transparency of customs procedures through the use of information technologies.</p> <p>Governments have an important role to play in addressing questions of trade policy and assuring the legal validity of documents in digital form.</p>

	Business action / observations	Government action required
3. Capacity building	Business is looking forward to working with governments to offer advice on how to coordinate capacity building efforts in developing countries' customs administrations. Business can do this by sitting on advisory committees created to formulate capacity building strategies.	<p>Strengthening and streamlining the trade facilitation environment in all countries will require capacity building in a number of developing countries; governments should examine existing programs of assistance and conduct a needs assessment to develop an assistance plan to improve the basic facilitation environment of all countries.</p> <p>This can be a collaborative effort with such organizations as the World Bank, the IMF, the WCO and the United Nations Conference on Trade and Development (UNCTAD).</p>

Intellectual property

Adequate protection of intellectual property rights in intangible assets in cyberspace is a top priority. This should be achieved through a balanced approach that protects both the rights of content providers and the interest of various other stakeholders in the digital networked environment.

	Business action / observations	Government action required
1. Copyright and neighbouring rights	<p>Technology is being developed to better track and protect copyrighted materials, and manage rights. Business is in dialogue with governments to ensure that copyright (including neighbouring rights) regimes are applied to the digital environment in a manner that promotes electronic commerce while protecting intellectual property rights.</p> <p>Business sectors are committed to cooperating to prevent, deter and respond to infringements that take place over digital networks, including the implementation of technical protection measures; the development of marketplace solutions such as licensing; cooperation with law enforcement; and refining procedures for promptly responding to notification or facts and circumstances from which infringing activity is apparent.</p> <p>Business will continue to provide information on the intellectual property implications of new technology.</p>	<p>WIPO adopted the Copyright and the Performances and Phonograms Treaties in December 1996. Governments should now move promptly to ratify and implement these treaties, taking into account the challenges and opportunities of the digital environment. The goal must be the establishment of a balanced and realistic framework of accountability that respects international norms; provides incentives for increased inter-industry cooperation to deter and respond to infringements; promotes responsible business practices; does not impose unreasonable burdens on intermediaries; and preserves an appropriate role for courts. Any legislation that deals with the applicability of copyright infringement liability rules should carefully examine how these rules apply to all stakeholders in the digital networked environment. Any framework that provides for limitations on liability for service providers should be restricted to damages and other monetary relief.</p> <p>Governments should consider further measures to secure property rights in the digital networked environment, including filling the gaps in protection for producers and performers of sound recordings left by the Performances and Phonograms Treaty.</p>

	Business action / observations	Government action required
2. Trademarks	Business has highlighted the problems raised by the discrepancy between the national scope of trademark laws and the international nature of electronic commerce and will work with WIPO to examine possible solutions. (See also Domain name system under Internet governance above).	Governments should work together at the international level in WIPO to ensure that national differences in trademark law and policy do not impede the trademark owner's ability to exploit and protect their trademarks in cyberspace.
3. Databases	Business is contributing to WIPO's work on this issue.	<p>Governments should ensure that any rights over databases should balance the interests of the creators of databases and the need to ensure the flow of and access to information.</p> <p>Governments should continue to work through WIPO towards adequate protection of intellectual property in databases.</p>

IV Annex - Selected industry self-regulatory initiatives

This annex provides examples of cross-company and joint business/government initiatives aiming to enhance trust in electronic commerce. Innovative schemes operated by individual companies are not included – although very often such proprietary efforts play a crucial role in heightening, through competition, standards of good business practice, this action plan is not the appropriate place to provide information on private initiatives. Finally, the annex is not meant to be an exhaustive list of initiatives but rather an attempt to demonstrate the rich variety of projects that the private sector is initiating to remove barriers to electronic commerce.

BBOOnline Reliability and Privacy Seal Program, Code of Online Business Practices

Bolero System

Business code of conduct from the Association of the Swedish IT and Telecom Industry

The Canadian Association of Internet Providers (CAIP) Code Of Conduct

The Canadian Association of Internet Providers (CAIP) Privacy Code

The Canadian Association of Internet Providers CAIP ISP Fair Practices

The Canadian Association of Internet Providers CAIP Protection Portal

Canadian Chamber of Commerce

CAP admark Scheme for UK Internet Advertising

CaseTrust Accreditation Scheme

Canadian Standards Association Model Code for the Protection of Personal Information

CBI Contractual Clauses and Group Policies

Code of Conduct for Electronic Commerce

Cybercrime Unit of ICC Commercial Crime Services

Dispute resolution for electronic commerce

ESOMAR Guideline on Conducting Marketing and Opinion Research Using the Internet and ESOMAR Guideline on Internet Privacy Policies and Privacy Statements

European Advertising Standards Alliance (EASA): Cross-Border Complaints System

European Electronic Signature Standardisation Initiative (EESSI)

Self-regulation for e-commerce marketing "The FEDMA's Ring of Confidence initiative"

General Usage for International Digitally Ensured Commerce (GUIDEC)

Guidelines for codes of practice for Internet Service Providers

Guidelines for transactions between virtual merchants and consumers

Guidelines for Electronic Direct Marketing

High assurance general ID-certificate with private key protected in an electronic ID-card

Hotlines Against Illegal Content

ICC Guidelines on advertising and marketing on the internet

International Content Rating Association (ICRA)

International DOI Foundation

International Online ADR

International Standardization of Online Trust Mark Programs

Internet One directory

New Zealand electronic Marketing Standards Authority (eMSA)

Online Ombuds Office

P3P

Paction – the model international sale contract application

PKI Assessment Guidelines

Standard Contractual Clauses for Transborder Dataflows

TradeCard

TRUSTe

TTP.NL

WebTrust

World Chambers Network (WCN)

Name of Initiative		BBBOnLine Reliability and Privacy Seal Program, Code of Online Business Practices
Objective		BBBOnLine was established to help build consumer trust and confidence in online commerce. The Reliability program seal assures that a company belongs to its local BBB; that it is an established business; has agreed to adhere to BBB standards of truthful advertising; and, has agreed to work with the BBB to resolve any disputes that may arise over its products or services. BBBOnLine Privacy offers a comprehensive assessment process to measure a company's ability to stand behind the promises made in its online privacy policy and offers a dispute resolution process for consumer privacy concerns. The Code of Online Business Practices is a guideline covering customer service and consumer protection issues for any online business.
Enforcement mechanism(s)		In both the Reliability and Privacy programs a company signs a license agreement committing to the principles of the program and the particular resolution process applicable to the program.
Leader(s) initiative	Issuing/ implementing organization(s)	BBBOnLine is part of the Council of Better Business Bureaus representing close to 400 major corporations and approximately 140 local Better Business Bureaus. The local bureaus have over 270, 000 business as part of their membership base.
	Supporting organization(s)	
[expected] Date of issuance / implementation		BBBOnLine Reliability was launched on 30 April 1997. BBBOnLine Privacy was launched on 17 March 1999.
Scope	General	Both programs are applicable to all businesses that are able to meet the standards and other criteria of the program.
	Sector	BBBOnLine Reliability is applicable to companies located in the United States and Canada. BBBOnLine Privacy is applicable to a company located anywhere in the world and has a reciprocal Japanese Privacy Seal in co-ordination with JIPDEC (the MITI sponsored Japanese Privacy Seal Authority.) BBBOnLine is working with organizations in different countries to build additional co-operative partnerships to address privacy and consumer protection issues.
	Geographic	
Examples of application		The BBBOnLine Reliability Program currently has over 10,000 participating websites. The BBBOnLine Privacy Program has over 800 approved websites with many more in the process.
Participation public sector		BBBOnLine works closely with the US Federal Trade Commission, State Attorney Generals and local law enforcement organizations if a fraudulent or scam type web site is identified. In developing the Privacy Program BBBOnLine worked closely with the Department of Commerce and Federal Trade Commission. The Council of Better Business Bureaus has a long successful history working closely with appropriate government organizations.
For full text/further information consult/contact		Ms. Mercedes Lemp Marketing Director BBBOnLine Inc. 4200 Wilson Boulevard Arlington, VA 22202 Tel 703 247 3661 Fax 703-276-8112 e-mail: mlemp@cbbb.bbb.org URL: www.bbbonline.org
Possible/expected evolution of the initiative		Goal is to partner with other organizations to develop a global approach to building consumer trust and confidence in online commerce.

Name of initiative		Bolero System
Objective		Facilitating international trade through a technical and legal infrastructure for electronic commerce
Enforcement mechanism(s)		Contract-based interfacing with domestic laws
Leader(s) initiative	Issuing/ implementing organization(s)	Bolero International Limited Bolero Association Limited
	Supporting organization(s)	Bolero-enabled partners listed at www.bolero.net
[expected] Date of issuance / implementation		September 1999
Scope	General	International trade
	Sector	Initial focus on shipping
	Geographic	Worldwide
Examples of application		Case studies appear at www.bolero.net . Users have realised substantial cost savings.
Participation public sector		Customs and other regulatory offices participate actively.
For full text/further information consult/contact		www.bolero.net
Possible/expected evolution of the initiative		Broadening focus to include an increasing number of trade transactions and instruments with both technical and legal support.

Name of initiative		Business code of conduct from the Association of the Swedish IT and Telecom Industry
Objective		The Association of the Swedish IT and Telecom Industry has issued seven business rules for their members. One of the rules regulates the following aspects of electronic information: <ul style="list-style-type: none"> • Distribution of inappropriate or abusive information • Respect of privacy and integrity • Electronic marketing and spamming • Transparency in pricing and other conditions
Enforcement mechanism(s)		Binding on members
Leader(s) initiative	Issuing/ implementing organization(s)	Association of the Swedish IT and Telecom Industry
	Supporting organization(s)	Confederation of Swedish Enterprise
Date of issuance / implementation		1997
Scope	General	Business-to-business and business-to-consumer
	Sector	--
	Geographic	--
Examples of application		650 member companies
Participation public sector		--
For full text/further information consult/contact		www.itforetagen.se
Possible/expected evolution of the initiative		--

Name of Initiative		The Canadian Association of Internet Providers (CAIP) Code Of Conduct
Objective		To govern the business conduct of ISPs as it relates to the public, public bodies and law enforcement officials.
Enforcement mechanism(s)		Voluntary adherence.
Leader(s) initiative	Issuing/ implementing organization(s)	The Canadian Association of Internet Providers (CAIP)
	Supporting organization(s)	Industry Canada
[expected] Date of issuance / implementation		October 1996
Scope	General	To assist ISPs with the development and implementation of internal policies and practices to comply with existing legal standards.
	Sector	Internet Service Providers
	Geographic	Canada
Examples of application		The Code will guide ISPs when they receive complaints about illegal content on web sites or network abuse.
Participation public sector		Industry Canada
For full text/further information consult/contact		www.caip.ca/caipcode.html
Possible/expected evolution of the initiative		CAIP is currently developing a "Fair Practices" guide for its ISP members that will, among other things, provide them with further direction regarding practical means and tools to comply with the Code of Conduct.

Name of Initiative		The Canadian Association of Internet Providers (CAIP) Privacy Code
Objective		To apply the principles of the Canadian Standards Association Model Code for the Protection of Personal Information to the online environment.
Enforcement mechanism(s)		Voluntary.
Leader(s) initiative	Issuing/ implementing organization(s)	The Canadian Association of Internet Providers
	Supporting organization(s)	Industry Canada
[expected] Date of issuance / implementation		September 1998
Scope	General	The CAIP Privacy Code is a voluntary code that represents a formal statement of principles and guidelines concerning the minimum protection that CAIP members will provide to their users regarding the protection of personal information. The Code applies to the management of personal information about a CAIP member's users in any form whether oral, electronic or written that is collected, used or disclosed by a member.
	Sector	Internet Service Providers
	Geographic	Canada
Examples of application		
Participation public sector		Ministry of Consumer and Commercial Relations (ON)
For full text/further information consult/contact		www.caip.ca/privacy.html
Possible/expected evolution of the initiative		CAIP is currently developing a "Fair Practices" guide for its ISP members that will, among other things, provide them with further direction regarding practical means and tools to comply with the CAIP Privacy Code.

Name of Initiative		The Canadian Association of Internet Providers CAIP ISP Fair Practices
Objective		To provide CAIP members with practical means to comply with CAIP's Code of Conduct and Privacy Code, and thereby promote consumer confidence in the use of the Internet.
Enforcement mechanism(s)		Voluntary.
Leader(s) initiative	Issuing/ implementing organization(s)	The Canadian Association of Internet Providers (CAIP).
	Supporting organization(s)	Industry Canada
[expected] Date of issuance / implementation		Launched 15 February 2001
Scope	General	To create modular action plans to help ISPs address issues relating to reputable delivery of service, content, privacy, security and unsolicited commercial email (spam).
	Sector	Internet Service Providers (ISPs)
	Geographic	Canada
Examples of application		The document will provide guidance to ISPs respecting procedures to follow when they receive complaints about illegal or objectionable content and the formation of contracts to be used with subscribers and web site owners.
Participation public sector		Industry Canada
For full text/further information consult/contact		www.caip.ca
Possible/expected evolution of the initiative		

Name of Initiative		The Canadian Association of Internet Providers CAIP Protection Portal
Objective		To provide a bilingual (English/French) public awareness web about Internet content issues for parents and consumers.
Enforcement mechanism(s)		N/A
Leader(s) initiative	Issuing/ implementing organization(s)	The Canadian Association of Internet Providers (CAIP).
	Supporting organization(s)	Industry Canada; Department of Justice
[expected] Date of issuance / implementation		25 February 2001
Scope	General	To contribute to the education of Internet users regarding illegal and offensive content on the Internet.
	Sector	General Public
	Geographic	Canada
Examples of application		The Portal profiles and provides links to Canadian organizations that have launched special initiatives to address Internet content issues.
Participation public sector		Industry Canada; Department of Justice
For full text/further information consult/contact		www.caip.ca/portal
Possible/expected evolution of the initiative		Additional profiles and links to be added as resources permit.

Name of initiative		Model Contractual Clauses for Transfer Of Personal Information to a Data Processor
Objective		To enable the transfer of personal data to third party service providers.
Enforcement mechanism(s)		<i>Personal Information Protection and Electronic Documents Act</i>
Leader(s) initiative	Issuing/ implementing organization(s)	Canadian Chamber of Commerce
	Supporting organization(s)	
Date of issuance / implementation		March 2002
Scope	General	Especially beneficial for SMEs.
	Sector	All
	Geographic	All
Examples of application		Transfer of personal data for payroll processing by third party service provider. Clauses can be directly inserted into existing contracts to assist the safeguarding of personal data being transferred to external suppliers.
Participation public sector		
For full text/further information consult/contact		Copies are available (Eng./Fr.) through the Canadian Chamber of Commerce by e-mailing: info@chamber.ca .
Possible/expected evolution of the initiative		

Name of Initiative		CAP admark Scheme for UK Internet Advertising (www.admark.org.uk)
Objective		A self-regulatory scheme for UK Internet advertising so that advertisers can declare to consumers their intention to advertise in a legal, decent, honest and truthful way. Those joining the scheme agree to comply with the British Codes of Advertising and Sales Promotion and the rulings of the Advertising Standards Authority. Main aims are to: <ul style="list-style-type: none"> - give consumers trust and confidence in Internet advertising, especially advertising in the admark scheme, and - inspire the confidence of governments, opinion formers and consumers in self-regulation for Internet advertising to ensure that new legislation on advertising is kept to a minimum.
Enforcement mechanism(s)		advertisers, agencies and the media comply with the British Codes of Advertising and Sales Promotion and rulings of the Advertising Standards Authority, backed up by legislation applied by the Office of Fair Trading (a government department) through the Control of Misleading Advertisements Regulations 2000 as amended to incorporate comparative advertising. Adjudications on complaints under the Codes are published weekly on the ASA website (www.asa.org.uk). The use of the CAP admark scheme does not indicate "approval" by either the ASA or CAP of the advertising material on the Internet. ASA will consider complaints against UK advertisers who are not in the scheme as well as against those who are in the scheme.
Leader(s) initiative	Issuing/ implementing organization(s)	The Committee of Advertising Practice
	Supporting organization(s)	The Advertising Standards Authority
Date of issuance / implementation		May 2001
	General	The British Codes of Advertising and Sales Promotion cover consumer-to-business and business-to-business non-broadcast advertising. The admark scheme is principally aimed at giving consumers confidence in business-to-consumer advertising.

Scope

	Sector	The admark scheme and the Codes apply to UK Internet advertising and the use of the scheme will enable companies to declare to consumers that the UK is their country of origin and that they will cooperate with the ASA and CAP in resolving complaints.
	Geographic	The UK Codes also cover the Isle of Man and the Channel Islands.
Examples of application		In 1998, ASA resolved 34 complaints about on-line ads, 6 required formal investigation and all of them were found to break the Codes, a further 8 presented smaller or clear-cut problems and were informally resolved.
For full text/further information consult/contact		Allan Chant, ASA/CAP 2 Torrington Place, London WC1E 7HW tel: 44-(0)20 7580 5555 Fax: 44-(0)20 7631 3051
Possible/expected evolution of the initiative		ASA is one of the 22 countries in the European Advertising Standards Alliance (see further in this annex). The scheme will also be recommended to the ICC for consideration in their discussion on the arbitration of complaints under its Internet Advertising Guidelines. The scheme has 18 founder members: MSN, Unilever, IBM, GlaxoSmithkline, Engage, 24/7, Egg, Nat West, Guardian Unlimited, Royal Mail, Yell, Nestle, Inspired Leaders, Nickelodeon, Hollinger Telegraph, Sainsbury, ANM and BT.

Name of Initiative		CaseTrust Accreditation Scheme
Objective		<ol style="list-style-type: none"> 1. To drive businesses to excellence through consumers through the declaration of good businesses practices and Fair Trading elements in-built in the criteria. 2. To profile businesses who are industry leaders who Go for CaseTrust Gold, a higher tier in the CaseTrust Accreditation Scheme overseas with our supporting organizations.
Enforcement mechanism(s)		<ul style="list-style-type: none"> - CaseTrust aims to address the assurance issue in e-commerce by making it compulsory for all e-commerce websites to have in place proper security and privacy systems in order to join the scheme. - Participating online businesses are also required to adopt a set of business practices such as respecting the privacy of customers' personal information. - Consumers can verify that the business is a genuine CaseTrust accredited business by referring to the online directory on the CASE website. - The CaseTrust qualifying criteria set out the minimum standards that retailers must comply with. Businesses who qualify for the scheme will be awarded the CaseTrust logo, which may then be displayed prominently on their websites or storefronts. - Checks will be conducted at random to ensure that the businesses practice what they preach. - In addition, all retailers will be subjected to periodic assessment to ensure that standards are maintained. CaseTrust offers redress to consumers who may be dissatisfied with their purchases. - If the matter is not resolved amicably within a reasonable period of time, it will then be brought up to the CASE mediation panel for resolution. The emphasis on dispute resolution and avoidance, also lays the ground for Fair Trading legislation.
Leader(s) initiative	Issuing/Implementing organization(s)	Consumers Association of Singapore (CASE)
	Supporting organization(s)	Infocomm Development Authority of Singapore Productivity and Standards Board Singapore Tourism Board
Date of issuance / implementation		End 1999, Re-launched in April 2001

Scope	General	
	Sector	On-line & physical storefronts
	Geographic	Singapore
Examples of application		
Participation public sector		NIL
For full text/further information consult/contact		CASE, CaseTrust Management Committee Ulu Pandan Community Building #05-01 170 Ghim Moh Road S297621 Tel: (65) 8751311 Fax: (65) 4637048 Email: casetrust@case.org.sg
Possible/expected evolution of the initiative		Internationalization of the scheme

Name of Initiative		Canadian Standards Association Model Code for the Protection of Personal Information
Objective		Addresses two broad concerns: the way in which organizations collect, use and disclose personal information; and the right of individuals to have access to personal information about themselves and to have the information corrected if necessary.
Enforcement mechanism(s)		Voluntary, but referenced by law or regulatory bodies in a variety of situations in Canada.
Leader(s) initiative	Issuing/ implementing organization(s)	Canadian Standards Association (CSA)
	Supporting organization(s)	Price Waterhouse - chair ITAC CBA Stentor American Express Public Interest Advocacy Centre Digital
[expected] Date of issuance / implementation		March 1996
Scope	General	Consumer -to-Business
	Sector	Transportation, Telecommunications, IT, Insurance, Health and Banking
	Geographic	Canada
Examples of application		Industry Canada - Jan 1998 - <i>The Protection of Personal Information</i> suggests using the CSA Model as a framework for Canadian legislation on privacy.
Participation public sector		Ministry of Consumer and Commercial Relations (ON) Industry Canada, Office of Privacy Commissioner Department of Justice, Heritage Canada
For full text/further information consult/contact		CSA 178 Rexdale Blvd. Toronto, Ontario M9W 1R3 Tel: (416) 747-2272/ Fax: (416) 474 2473 Grant Gillis, Project Manager, Quality Program grant.gillis@csa.ca www.csa.ca
Possible/expected evolution of the initiative		

Name of initiative		CBI Contractual Clauses and Group Policies
Objective		To enable transfers of personal data to countries outside the EEA
Enforcement mechanism(s)		Via obligations and warranties
Leader(s) initiative	Issuing/ implementing organization(s)	CBI
	Supporting organization(s)	
[expected] Date of issuance / implementation		Shared with but not approved by UK Information Commissioner and European Commission.
Scope	General	
	Sector	All sectors
	Geographic	All countries
Examples of application		To ensure adequate protection for personal data being transferred from a subsidiary company in the EEA to a parent company outside the EEA.
Participation public sector		
For full text/further information consult/contact		Copies available to CBI members from CBI Information Centre +44 207 395 8247
Possible/expected evolution of the initiative		

Name of initiative		Cybercrime Unit of ICC Commercial Crime Services
Objective		To investigate, collate & disseminate information to the industry on all matters relating to commercial cybercrime
Enforcement mechanism(s)		None
Leader(s) initiative	Implementing organization(s)	ICC Commercial Crime Services
	Supporting organization(s)	
(Expected) Date of issuance/implementation		01/01/2000
Scope	General	Commercial Crime & Malpractice Internet & Corporate Networks
	Sector	Non-sector specific
	Geographic	Worldwide
Examples of application		Closed down sites offering fraudulent financial proposals, providing a monthly bulletin on cyber crime, advising clients on wireless network vulnerabilities
Participation public sector		Yes, works closely with Government Agencies and Law Enforcement.
For full text/further information Consult/contact		P Mukundan, Director, ICC-Commercial Crime Services p.mukundan@icc-ccs.org.uk
Possible/expected evolution of the Initiative		To become a focal point for business in respect of information regarding Commercial cybercrime.

Name of initiative		Code of Conduct for Electronic Commerce
Objective		To draft a framework with a minimum set of rules for model behaviour, which might gain commitment of all parties involved in electronic commerce and thus attribute to the process of building trust and confidence. The general principles Transparency, Reliability and Confidentiality and privacy have been taken as a starting point.
Enforcement mechanism(s)		Contractually binding for subscribers, possibly agreements on private-law settlement of disputes. Certification will possibly be another way of enforcement.
Leader(s) initiative	Issuing/ implementing organization(s)	The Dutch Electronic Commerce Platform (ECP.NL).
	Supporting organization(s)	the Confederation of Netherlands Industry and Employers (VNO-NCW), individual companies, the Dutch consumer organization Consumentenbond, as well as the Economic Affairs Department and the Justice Department.
[expected] Date of issuance / implementation		The current version (4.0) of the Model Code of Conduct for Electronic Business was launched late October 2001
Scope	General	Business-to-business; Business-to-consumer, Business-to-administration
	Sector	All sectors
	Geographic	No limits
Examples of application		The Model Code of Conduct for Electronic Business is explicitly mentioned as an example in the Centre for Trade Facilitation and Electronic Business of the United Nations (UN/CEFACT) recommendation regarding E-commerce self-regulatory instruments. The leading Dutch trustmark 'Webtrader', which ceased to exist at the beginning of 2002, was based on the Model Code of Conduct. It's successor 'Thuiswinkel Waarborg' is also based on the Model Code of Conduct. Numerous organizations have adopted Codes of Conduct for their e-business activities, which have been inspired by the Model Code of Conduct.
Participation public sector		See "Supporting organizations"
For full text/further information consult/contact		Ton Wagemans (ton.wagemans@ecp.nl) Bart Schermer (bart.schermer@ecp.nl)
Possible/expected evolution of the initiative		By the end of February an initiative will be launched to help branches of trade implement the provisions of the Model Code of Conduct within their branch This initiative is a joint effort of ECP.NL and Syntens, an innovation network for employers.

Name of initiative		Dispute resolution for electronic commerce
Objective		ICC offers a variety of high-speed, low-cost methods for resolving electronic commerce disputes through arbitration under the 1998 ICC Rules of Arbitration; Fast-track arbitration under the 1998 rules; ICC ADR Rules and ICC Rules for Expertise
Enforcement mechanism(s)		After voluntary incorporation into a contract an arbitration clause becomes binding upon the parties. Pursuant to various treaties (i.e. the New York Convention), arbitral awards are enforceable in signatory states. Amicable dispute resolution mechanisms may be appropriate vehicles for the enforcement of self-regulatory guidelines, codes and practices.
Leader(s) initiative	Issuing/ implementing organization(s)	ICC (International Chamber of Commerce) through its ICC Dispute Resolution Services
	Supporting organization(s)	
[expected] Date of issuance / implementation		ICC arbitration rules in effect since 1 January 1998. New ICC ADR rules in effect since 1 July 2001. ICC Rules for Expertise under revision but current version in force since 1 January 1993.
Scope	General	Mostly business-to-business, but consumer-to-business disputes are not excluded.
	Sector	Non sector-specific.
	Geographic	International
Examples of application		
Participation public sector		None
For full text/further information consult/contact		www.iccarbitration.org Emmanuel Jolivet, +33-1-49532943
Possible/expected evolution of the initiative		ICC dispute resolution mechanisms will continue to evolve to meet business needs in electronic commerce and generally.

Name of initiative		ESOMAR Guideline on Conducting Marketing and Opinion Research Using the Internet and ESOMAR Guideline on Internet Privacy Policies and Privacy Statements
Objective		To outline the main principles which must be followed in carrying out research on (or about) the Internet and in reporting the findings of such research with the objective to protect the interests both of Internet respondents and of the users of Internet research findings.
Enforcement mechanism(s)		Complaints procedures through ESOMAR. This guideline is based on the principles of the ICC/ESOMAR International Code of Social and Marketing Research which has been undersigned by all ESOMAR members, the management of more than 1000 research institutes with ESOMAR members and by 102 associations in 51 countries worldwide.
Leader(s) initiative	Issuing/ implementing organization(s)	ESOMAR
	Supporting organization(s)	World Federation of Advertisers (WFA), Advertising Research Foundation (ARF)
Date of issuance / implementation		ESOMAR 2000: ESOMAR Guideline on Conducting Marketing and Opinion Research Using the Internet ESOMAR 2001: ESOMAR Guideline on Internet Privacy Policies and Privacy Statements
Scope	General	Business-to-consumer and business-to-business
	Sector	Market, opinion and social research
	Geographic	Worldwide
Examples of application		

Participation public sector	
For full text/further information consult/contact	Www.esomar.nl or i.vandermeersch@esomar.nl
Possible/expected evolution of the initiative	Will be updated regularly as needed. Next up-date to be available in 2002 (ESOMAR Guideline on Conducting Marketing and Opinion Research Using the Internet)

Name of Initiative		European Advertising Standards Alliance (EASA): Cross-Border Complaints System
Objective		<p>The key objectives of the EASA's development of self-regulation for the Internet are:</p> <ul style="list-style-type: none"> a) To provide effective channels for the resolution of cross border complaints about advertisements; b) To develop high Internet standards through best advertising practice to give consumers confidence and trust in the advertisements they access; c) To give national, European and International Governments, consumer bodies and opinion formers confidence in the advertising industry's self-regulatory systems to keep the need for legislation to a minimum.
Enforcement mechanism(s)		National self-regulatory systems for advertising
Leader(s) initiative	Issuing/ implementing organization(s)	EASA Internet Working Group/ National Self-regulatory Organizations
	Supporting organization(s)	EASA Members – Self-regulatory Organizations - European Industry Associations
[expected] Date of issuance / implementation		(July 1999 – issued to advertising industry bodies for consultation/feedback) Issuance expected in 2000
Scope	General	National self-regulatory codes/principles. The existing national self-regulatory systems for advertising in the EASA member countries
	Sector	Advertising/Commercial Communications
	Geographic	<p>The EASA has 38 members.</p> <p>28 of these are self-regulatory bodies (SROs), and comprises of 22 European countries, including all European Union (EU) Member States, as well as four corresponding members in Canada, South Africa, New Zealand and the US. These members apply codes/principles of advertising practice which are based on those drawn up by ICC.</p> <p>EASA has since November 2001 accepted industry associations supporting self-regulation into membership. Currently there are 10 organizations in membership representing advertisers, agencies, and the media.</p> <p>EASA is now the single authoritative voice for the European advertising industry on self-regulation.</p>
Examples of application		<p>The EASA established a cross border complaint procedure in 1992, and this has now been extended to co-ordinate consumer complaints about the content of electronic advertisements. The procedure is based on the country of origin principle, as prescribed in the EU Television Without Frontiers (Broadcasting) Directive (97/36/EC) and applies to complaints from one member country about advertisements that originate in another. These procedures are applicable for Internet advertising as self-regulation, backed up where appropriate by nationally based legislation, is seen to be the most appropriate and effective measure to provide protection for consumers while enabling commerce to flourish. To date the cross-border complaints system has closed a number of Internet complaints.</p>

	The EASA has encouraged self-regulatory bodies (SROs) in membership to receive complaints online and provides a means via the EASA website for consumers to make online complaints which will be forwarded to the SRO in the country of origin.
Participation public sector	National organizations and EU
For full text/further information consult/contact	Dr Oliver Gray Director-General European Advertising Standards Alliance 10A Rue de la Pépinière B - 1000 Brussels Belgium Tel.: (+32 2) 513 78 06 Fax: (+32 2) 513 28 61 E-mail: library@easa-alliance.org
Possible/expected evolution of the initiative	This will contribute to a wider evaluation of internet advertising and cross-border complaints handling with the advertising industry, and to the stimulation of discussions that will aid our understanding and further develop the practice and application of advertising self-regulation on a global level within the context of interactive new media.

Name of initiative		European Electronic Signature Standardization Initiative (EESSI)
Objective		<p>Industry initiative under the ICT Standards Board with the support of the two European standardization bodies, CEN and ETSI, to provide implementation frameworks in support of the European Directive on Electronic Signature.</p> <p>Such frameworks should be built upon international standards and other form of voluntary agreements which can be used to provide legally recognized signatures not only across Europe, but at global level through international cooperation.</p> <p>The ultimate objective is the publication by CEN and ETSI and recognition by the European Commission of industry agreed documents, relating to the technical infrastructure and self-regulatory guidelines for certification authorities and the like. Some documents could ultimately become European standards.</p>
Enforcement mechanism(s)		Compliance with the minimal legal framework stated by the European Directive
Leader(s) initiative	Issuing/ implementing organization(s)	EESSI Steering Group, CEN; ETSI
	Supporting organization(s)	ICT Standards Board ,CEN, ETSI
[expected] Date of issuance / implementation		<p>1st step (assessment of existing standards, standardization needs in light of market requirements, proposals for action) achieved (July 99).</p> <p>2nd step (work programme) first set of standards focusing on the use of PKI technologies for electronic signature in support of the implementation of the European Directive (April 01).</p> <p>3rd step (work programme) standards for the specifications for other classes of electronic signature (in progress)</p>
Scope	General	Legal recognition of electronic signature in the open electronic commerce environment
	Sector	Non sector specific
	Geographic	1 st priority European Union (domain of application of the European Directive), overall objective: international.
Examples of application		e-Commerce
Participation public sector		European Commission, EU Member States
For full text/further information consult/contact		1 st step Final Report available on http://www.ict.etsi.org/eessi/EESSI-homepage.htm/
Possible/expected evolution of the initiative		Consult http://www.ict.etsi.org/eessi/EESSI-homepage.htm

Name of initiative		Self-regulation for e-commerce marketing "The FEDMA's Ring of Confidence initiative"
Objective		<ul style="list-style-type: none"> To enhance consumer trust and confidence on electronic commerce; To promote best business practices for electronic commerce & therefore promote the growth of e-commerce in Europe. <p>These objectives would be achieved through the implementation of several key elements which take into full consideration present consumer concerns: European Code of Conduct, European Guarantee Seal, Enforcement Mechanisms, Monitoring and Surveillance, Specific Software tools, specific services and awareness campaign.</p>
Enforcement mechanism(s)		The review of the FEDMA Code started in July 2001. One of the objectives of the review Task Force will be to set up enforcement Committee.
Leader(s) initiative	Issuing/ implementing organization(s)	Federation of European Direct Marketing, FEDMA
	Supporting organization(s)	National Direct Marketing Associations in Europe
[expected]	Date of issuance / implementation	Mid 2003
Scope	General	Business-to-consumer
	Sector	Any company having a web site
	Geographic	No geographic boundaries: the Internet
Examples of application		<ul style="list-style-type: none"> The FEDMA Code of conduct for Electronic Commerce and Interactive Marketing was unanimously adopted by the members of the FEDMA board on 5 September 2000. FEDMA is currently working on a Data Protection Code, which should be completed by March 2002 FEDMA is working on the concept of a common set of standards and a seal to arrive at a common and compatible infrastructure for handling cross-border consumer disputes in the EU and North America. FEDMA will advance this concept in alliance with BBBOnline, and Eurochambres The Consumer Complaints Resolution Mechanism project (CCRM) aims to encourage trust and confidence in e-commerce with the creation and the development of a multilingual and interactive complaint form. This project will develop specified software tool for business to Consumer issues and will focus on a large awareness campaign <p>For more information, please follow this link: http://www.fedma.org/code/page.cfm?id_page=74#liens05</p>
Participation public sector		Only in funding
For full text/further information consult/contact		Alastair Tempest: atempest@fedma.org
Possible/expected evolution of the initiative		The whole project could be developed internationally through the International Federation of Direct Marketing Associations (IFDMA).

Name of initiative		General Usage for International Digitally Ensured Commerce (GUIDEC)
Objective		A set of common definitions and business-generated best practices for certifying and "ensuring" electronic commerce to: <ul style="list-style-type: none"> • facilitate further development of solutions to security • identify problems in electronic commerce over the Internet • Act as a unifying or starting point for some of the diverging policy approaches.
Enforcement mechanism(s)		Voluntary.
Leader(s) initiative	Issuing/ implementing organization(s)	ICC (International Chamber of Commerce)
	Supporting organization(s)	
Date of issuance / implementation		November 1997, revised in 2001
Scope	General	Business-to-business
	Sector	Non sector-specific.
	Geographic	International
Examples of application		GUIDEC has been widely referred to in the press and by industry as a unique reference for industry best practices and harmonized definitions. It has also been used by UNCITRAL as reference material for its work on electronic signatures.
Participation public sector		None
For full text/further information consult/contact		http://www.iccwbo.org Ayesha Hassan, +33-1-49533013
Possible/expected evolution of the initiative		Will be updated in 2003

Name of initiative		Guidelines for codes of practice for Internet Service Providers
Objective		This guideline consists of 7 Chapters, 20 articles and 2 additional rules. The objective of this guideline is to protect users (including minors) and to realize the sound development of Internet Connection Services by the members of Telecom Services Association of Japan by responding appropriately to various problems (illegal or harmful content etc.) arising from providing Internet Connection Services.
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	Telecom Services Association of Japan (TELESA)
	Supporting organization(s)	
[expected] Date of issuance / implementation		16 February 1998
Scope	General	Business-to-business; Business-to-consumer; Generic
	Sector	Internet Service Providers, Telecommunications Carriers
	Geographic	Japan
Examples of application		The association consists of 388 enterprises.
Participation public sector		
For full text/further information consult/contact		http://www.telesa.or.jp/e_guide/e_guid01.html
Possible/expected evolution of the initiative		The Guidelines will be reviewed continuously to ensure its efficacy as a guiding principle for members of the Association.

Name of initiative		Guidelines for Electronic Direct Marketing
Objective		Electronic commerce targeting consumers in Japan
Enforcement mechanism(s)		Compulsory to the JADMA members
Leader(s) initiative	Issuing/ implementing organization(s)	Japan Direct Marketing Association(JADMA)
	Supporting organization(s)	Ministry of Economy, Trade and Industry
[expected] Date of issuance / implementation		19 th January, 1999
Scope	General	Business-to-consumer
	Sector	Non sector-specific
	Geographic	Japan
Examples of application		The examples as yet
Participation public sector		
For full text/further information consult/contact		http://www.JADMA.org jadma@JADMA.org
Possible/expected evolution of the initiative		will be amended as needed

Name of initiative		Guidelines for transactions between virtual merchants and consumers
Objective		To promote the sound and healthy development of EC, these guidelines have been adopted as policies aimed at companies and designed to make transactions fair and protect the consumer, with the emphasis on preventing trouble before it occurs.
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	Electronic Commerce Promotion Council of Japan (ECOM)
	Supporting organization(s)	
[expected] Date of issuance / implementation		March 1999
Scope	General	Business-to-consumer
	Sector	Internet shopping
	Geographic	International
Examples of application		
Participation public sector		
For full text/further information consult/contact		http://www.ecom.jp/ecom_e info@ecom.jp
Possible/expected evolution of the initiative		Will be updated regularly as needed

Name of initiative		Guidelines for Use of Smart Cards (contact/contactless)
Objective		Targeting shops, businesses, and operation companies expected introduce smart cards and systems, these guidelines address a cross section of items to be examined and information required in the course of introducing such systems. They address the conceivable fields or situations of application and provide specific content related to those fields and situations. Overall, this report amounts to an effort to promote and facilitate the use of smart cards.
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	Electronic Commerce Promotion Council of Japan (ECOM)
	Supporting organization(s)	
[expected] Date of issuance / implementation		March, 1998
Scope	General	Business-to-consumer
	Sector	Non sector-specific
	Geographic	International
Examples of application		
Participation public sector		
For full text/further information consult/contact		http://www.ecom.jp/ecom_einfo@ecom.jp
Possible/expected evolution of the initiative		Developed to the Guidelines for Building IC Card Terminal Infrastructures, released in March 2000.

Name of initiative		Guidelines on Personal Information Protection in Electronic Commerce in the Private Sector
Objective		To ensure the sound development of electronic commerce, all enterprises or individual businessmen that handle personal data of consumers in electronic commerce must take measures to protect these data. These guidelines have been prepared for the purpose of protecting personal data handled in electronic commerce.
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	Electronic Commerce Promotion Council of Japan (ECOM)
	Supporting organization(s)	
[expected] Date of issuance / implementation		March 1998
Scope	General	Business-to-consumer
	Sector	Non sector-specific
	Geographic	Japan/International
Examples of application		
Participation public sector		
For full text/further information consult/contact		http://www.ecom.jp/ecom_einfo@ecom.jp
Possible/expected evolution of the initiative		Will be updated regularly as needed

Name of initiative		High assurance general ID-certificate with private key protected in an electronic ID-card
Objective		Co-operation between public and private sector in order to facilitate common rules for strong authentication, use of digital signatures and strong encryption during transport of data. These three basic security services can be used for electronic commerce as well for governments' need for a "single face to citizen"
Enforcement mechanism(s) Need for interoperability		Voluntary by members of the non profit organization Certifications by the organization until national standardization decisions are made.
Leader(s) initiative	Issuing/ implementing organization(s)	SEIS – Secured Electronic Information in Society (A non-profit organization with c 60 organizations from both private and public sectors).
	Supporting organization(s)	GEA – Swedish Alliance for electronic business
[expected] Date of issuance / implementation		Technical specifications and a Certification Policy (16/06/98). Partly implemented by banks and the Swedish Post
Scope	General	Generic. All specification published via the net. Free to be used.
	Sector	
	Geographic	Sweden
Examples of application		First used in the finance sector for Internet Banking and other payment instructions. Public catalogue services not yet available. > 50 000 users.
Participation public sector		Members of SEIS
For full text/further information consult/contact		gea@gea.ihb.se www.gea.nu
Possible/expected evolution of the initiative		The general ID-certificate can be used for applications of any other certificate belonging to other PKI-schemes (e.g. SET Certificates, email certificates etc)

Name of initiative		Hotlines against illegal content, child pornography, and racism/discrimination on the Internet
Objective		Reports to these hotlines result in swift action against the reported illegal content, where necessary in cooperation with public official an/or police. In addition to being illegal, illegal content has a strong negative impact on Internet in general and specifically on the trustworthiness of the medium.
Enforcement mechanism(s)		Voluntary. Working on formal public-private partnership.
Leader(s) initiative	Issuing/ implementing organization(s)	NLIP is the Dutch ISPA (ISPA-NL): Internet Service Providers Association Netherlands
	Supporting organization(s)	Government, police
[expected] Date of issuance / implementation		Operational for 3 years now
Scope	General	All citizens and companies can report
	Sector	Internet
	Geographic	Netherlands
Examples of application		Many reports made to each hotline. See for instance yearly report (in English) at http://www.meldpunt.org/
Participation public sector		Law department, department of the interior, police
For full text/further information consult/contact		http://www.nlip.nl/ http://www.meldpunt.org/ mailto:hans.leemans@nlip.nl (president/CEO NILP)
Possible/expected evolution of the initiative		Organizational links being made to other European and global initiatives, cooperation with public authorities developing. Illegal content hotline will be developed

Name of initiative		ICC Guidelines on advertising and marketing on the internet
Objective		Guidelines proposing standards for ethical conduct of advertisers and marketers offering goods and services over Interactive Media to increase the public's confidence in marketing in the interactive media, to safeguard advertisers' freedom of expression, to minimize the incentive for governmental regulation, and to meet reasonable consumer privacy expectations.
Enforcement mechanism(s)		Like ICC's other marketing codes, the Internet guidelines are voluntary but serve as a global reference point for principles of ethical behaviour by companies world-wide. They are of a general nature so that national and sector-specific rules can build on them.
Leader(s) initiative	Issuing/ implementing organization(s)	ICC (International Chamber of Commerce)
	Supporting organization(s)	
[expected] Date of issuance / implementation		2 April 1998
Scope	General	The Guidelines set standards of ethical conduct to be observed by all involved with advertising and marketing activities on the Internet.
	Sector	Non sector-specific
	Geographic	International
Examples of application		The Guidelines serve as a basis for many self-regulatory e-advertising schemes currently being set up (some examples can be found in this Annex). They have been endorsed by over 100 companies and associations, and supported by the Global Business Dialogue for Electronic Commerce.
Participation public sector		None
For full text/further information consult/contact		http://www.iccwbo.org ICC, +33-1-49532827
Possible/expected evolution of the initiative		Will be updated regularly as needed

Name of initiative		International Content Rating Association (ICRA)
Objective		Our mission is to develop, implement and manage an internationally acceptable voluntary self-rating system which provides Internet users world wide with the choice to limit access to content they consider harmful, especially to children.
Enforcement mechanism(s)		Every content provider must agree to terms and conditions stating that they have not willfully misrepresented themselves. In addition, every site is visited, spot checks undertaken and full audit of sites conducted. An automated web crawler visits every site to check for label integrity. We also respond to comments, complaints and suggestions from the general public.
Leader(s) initiative	Issuing/ implementing organization(s)	Internet Content Rating Association.
	Supporting organization(s)	ICRA members include: Bell Canada, Internet Watch Foundation, T-Online International AG, Microsoft Corporation, Bertelsmann Foundation, IBM, NetMom, Cable & Wireless, Thus PLC, AOL Europe, Internet Association Japan, BT Openworld, AOL Inc, Childnet International, VeriSign, Digimarc Corporation, PAGi, Kids Domains, Inc, Verizon, Yahoo! Inc
Date of issuance / implementation		December 2000 onwards
Scope	General	The rating system is used by both content providers to self-rate their sites and by parents and other users to block potentially harmful material within their browsers.

	Sector	The system is applicable to all sectors in all parts of the world. Commercial, educational, government, military and personal sites have all rated with ICRA.
	Geographic	Global
Examples of application		Over 50,000 sites worldwide have rated with ICRA. ICRA will launch ICRAfilter in Q1 2002.
Participation public sector		ICRA has worked closely with government departments and agencies all over the world. Meetings have been held with the US Dept of Commerce, OECD, the Australian Broadcasting Authority and the European Commission amongst others.
For full text/further information consult/contact		Stephen Balkam; CEO, Internet Content Rating Association, 22 Old Steine, Brighton, East Sussex, BN1 1EL, United Kingdom. Telephone: +44 (0) 1273 648 332, admin@icra.org and David Kerr; Secretary General; Internet Content Rating Association; 5 Coles Lane; Oakington, Cambridge CB4 5BA; UK; +44 (1223) 23 7700; chief@iwf.org.uk
Possible/expected evolution of the initiative		ICRAfilter to be launched in March 2002

Name of initiative		International DOI Foundation
Objective		<p>To support the needs of the intellectual property community in the digital environment, and specifically to promote and develop the use of the Digital Object Identifier.</p> <p>The Digital Object Identifier (DOI®) is a system for interoperably identifying and exchanging intellectual property in the digital environment. It provides an extensible framework for managing intellectual content in any form at any level of granularity. The International DOI Foundation (IDF), a non-profit organization, manages development, policy, and licensing of the DOI to registration agencies and technology providers and advises on usage and development of related services and technologies.</p> <p>The IDF utilizes CNRI's Handle technology (www.handle.net) and a structured metadata component based on the EC-supported indecs project (www.indecs.org; IDF is one of the two bodies managing the indecs intellectual property rights). The DOI "application profile" integrates CNRI's digital object architecture and technology with well-structured metadata in order to provide a coherent and consistent means of expressing interoperable metadata and resolvable identifiers in a digital environment.</p> <p>The IDF are supporting further developments such as the extension of the successful indecs project further into rights management.</p>
Enforcement mechanism(s)		Policies and procedures defined in the DOI handbook. Issuance of a DOI requires conformance with the Foundation's rules. An implementation of the Uniform Resource Name/ Uniform Resource Identifier specification as defined by the IETF and W3C. Conformance to standard syntax and other rules laid down by the Foundation and where appropriate formalized as international standards.
Leader(s) initiative	Issuing/ implementing organization(s)	The International DOI Foundation (www.doi.org)

	Supporting organization(s)	The Foundation is an open consortium that any organization may join. Financial support for the DOI system is provided by members until such time as the network of DOI Registration Agencies can be self-funding. Current members: see http://www.doi.org/idf-member-list.html Prefix holders (organizations able to assign DOIs): see http://www.doi.org/prefix_holders.html Registration Agencies (organizations able to empower others to assign DOIs): see http://www.doi.org/registration_agencies.html Underlying technologies: indecs (www.indecs.org); handle (www.handle.net); CNRI (www.cnri.reston.va.us)
[expected] Date of issuance / implementation		DOIs have been issued since October 1998. The DOI system is currently actively implemented by many publishers including over 70 through the CrossRef consortium (www.crossref.org)
Scope	General	Intellectual property rights owners and users
	Sector	Non sector-specific
	Geographic	World
Examples of application		Persistent identification of entities in the intellectual property system, e.g. textual abstractions (works), tradable items (digital and physical files); licensable items (e.g. performances), etc.
Participation public sector		Open
For full text/further information consult/contact		Web site: www.doi.org Contact person: Norman Paskin, Director, International DOI Foundation PO Box 233; Kidlington, Oxford; OX5 1XU; U.K.; Tel: (+44) 1865 843798; Fax: (+44) 1865 843446; E mail: n.paskin@doi.org
Possible/expected evolution of the initiative		Application of DOIs in other sectors beyond initial text implementations. Further development of the DOI system in collaboration with existing standard mechanisms for identification and metadata. IDF is currently supporting work to extend the indecs analysis into both the rights transaction and identity management (party identifiers) areas. Appointment of multiple registration agencies and further application development. Development of standard tools for multiple resolution of identifiers.

Name of initiative		International Online ADR
Objective		To propose making dispute resolution procedures that suit to the international market and necessary conditions of dispute resolution organizations in order to maintain online trust mark authority and secure mark's effectiveness. (For an accomplishment of this objective, to get market needs and verify effectiveness of dispute resolution mechanism)
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	Electronic Commerce Promotion Council of Japan (ECOM) Korea Institute for Electronic Commerce (KIEC) BBBOnline
	Supporting organization(s)	Electronic Commerce Promotion Council of Japan (ECOM)
[expected] Date of issuance / implementation		January 2002
Scope	General	Business-to-consumer
	Sector	Internet shopping
	Geographic	Japan, Korea, USA, Canada
Examples of application		Net shopping dispute resolution service
Participation public sector		
For full text/further information consult/contact		http://www.ecom.jp/adr/
Possible/expected evolution of the initiative		Will be updated as needed

Name of initiative		International Standardization of Online Trust Mark Programs
Objective		Global promotion of the mark program and creating awareness, promotion of international trade, standardization of online business criteria and enhancing the added values for mark granted businesses, setting of the international common logo mark, development of interoperable dispute resolution procedures and technology that supports them, and building a cooperative system among dispute resolution organizations.
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	Global Trust Mark Alliance
	Supporting organization(s)	Electronic Commerce Promotion Council of Japan(ECOM)
[expected] Date of issuance / implementation		March, 2003
Scope	General	Business-to-consumer
	Sector	Internet shopping
	Geographic	Member countries of the Alliance
Examples of application		Online shopping mark
Participation public sector		
For full text/further information consult/contact		http://www.ecom.jp/ecom_e http://mark.cin.or.jp/ http://www.jadma.org/ost/index.html
Possible/expected evolution of the initiative		Will be updated as needed

Name of initiative		Internet One
Objective		Provide identification of legitimate Internet trading companies through an authoritative listing facility associating trademarks; brand names, company names, telephone numbers, directly with internet addresses, URLs, IP addresses and domain names, irrespective of the country code top level domains or generic top level domains in which registration has been effected. Correlating "real world" identifiers with those of the "virtual world" gives consumers greater certainty that the entity known to them in the real world is indeed that visible to them in the virtual world. Legitimate Internet traders register their details against a nominal charge through a recognized domain name registrar, Internet service web hosting company, certification authority, PTT operator or with IN ONE directly. Users may retrieve registered information, free of charge, using any standard Internet browser, entering in the address line of the browser the requisite trademark/company name/telephone nr, followed by ".io" to be referred directly to the registered Internet site. Where multiple identical trademarks/brandnames/company names are entered, the IN ONE system automatically generates a directory style listing from which the user may distinguish and select their desired company/destination. IN ONE will warn consumers within about 4 seconds of being notified of the potential infringement that the goods or services may be imitations of their reputable namesakes. IN ONE leaves the determination of who is a legitimate trader up to specialized agencies.
Enforcement mechanisms		On-line dispute resolution/arbitration facilities (http://internetONE.wipo.int) National courts

Leader(s) initiative	Issuing/ implementing organization(s)	Internet ONE Research Institute for Computer Science World Intellectual Property Organization
	Supporting organization(s)	Council of Internet Domain Name Registrars World Chambers of Commerce Network Electronic Commerce Associations
[expected] Date of issuance / implementation		Current
Scope	General	Business-to-business and business-to-consumer
	Sector	Non sector-specific
	Geographic	Global
Examples of application		IN ONE is the only authoritative directory on the Internet today using pioneering technology to a non-proprietary platform.
Participation public sector		Group of Eight Industrialized Nations, Government of Australia, France, Germany, Korea, Soviet Union, UK, USA and European Commission.
For full text/further information consult/contact		http://www.io.io Internet ONE P.O. Box 4040 Christchurch Dorset BH23 1XW Fax 44 1202 430 580
Possible/expected evolution of the initiative		IN ONE is seeking additional strategic partners from all nations and field of e-commerce. Designed in the UK, IN ONE and its partners have servers and infrastructure in New York, London, Amsterdam, Tokyo and Melbourne and already just under 100 partners from 23 countries. Readers of various Internet magazines voted IN ONE "best consumer customer service" at the recent European Internet Industry Awards 1999.

Name of initiative		The Online Trust Mark System for Winning Trust for Electronic Commerce
Objective		To help consumers avoid trouble with false or deceptive EC merchants. The seal of approval are displayed on the homepages of EC merchants known to be engaged in legitimate business.
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	Japan Chamber of Commerce and Industry Japan Direct Marketing Association
	Supporting organization(s)	Electronic Commerce Promotion Council of Japan(ECOM)
[expected] Date of issuance / implementation		September 1999
Scope	General	Business-to-consumer
	Sector	Internet shopping
	Geographic	Japan(For the shops whose headquarters are in Japan)
Examples of application		Online shopping mark
Participation public sector		
For full text/further information consult/contact		http://www.ecom.jp/ecom_e http://mark.cin.or.jp/ http://www.jadma.org/ost/index.html
Possible/expected evolution of the initiative		Will be updated as needed

Initiative		New Zealand electronic Marketing Standards Authority (eMSA)
Objective		Maintains a self-regulatory certification and adjudication scheme for internet advertising and consumer complaint resolution in New Zealand. Advertising Codes of Practice administered by the New Zealand Advertising Standards Authority and the Code of Ethics of the New Zealand Direct Marketing Association will be applied to ensure consumer and governmental confidence in a self-regulatory system to maintain standards in Advertising on the Internet. The certification process will include requirements of the advertiser seeking certification as to the delivery of products and services offered and the availability of dispute resolution mechanisms for the benefit of the consumer.
Enforcement Mechanism(s)		Voluntary agreements between advertisers, agencies, print and electronic media and New Zealand based internet service providers to observe standards required by the Fair Trading Act and related consumer protection legislation together with the Advertising Standards Authority Voluntary Codes of Advertising Practice the Code of Ethics of the New Zealand Direct Marketing Association. The agreement will require the advertiser to accept the jurisdiction of eMSA in determining consumer complaints arising from products and services purchased from the internet once the advertisers' internal dispute resolution procedures have been exhausted. The implementation of a verification programme modeled in the UK 'Trustmark' scheme. The scheme will be promulgated by eMSA. ASA and eMSA decisions will be published on the eMSA website, supplemented by the dissemination (free of charge) of written decisions to the media, government bodies, advertisers and advertising agencies. Certification will not extend to the content of any advertisement or the conduct of the advertiser. This is the rationale for the separation of the certification body and the adjudication body. New Zealand experience indicates that publicity provides the most effective method of enforcement of standards but it is also intended to seek agreement of internet service providers to remove sites containing offending material and to develop cross-border alliances to achieve effective enforcement.
Leader(s) Initiative	Issuing Implementing Organization	New Zealand electronic Marketing Standards Authority
	Supporting Organization(s)	The New Zealand Advertising Standards Authority; New Zealand Direct Marketing Association; The New Zealand Chambers of Commerce; The Ministry of Consumer Affairs; ICC New Zealand National Committee of Advertising, Marketing & Distribution; Association of New Zealand Advertisers; Communication Agencies Association of New Zealand
Date of Issuance		May 2001
Scope	General	Business to consumer primarily, business to business secondary
	Sector	All
	Geographic	New Zealand with cross-border alliances
Examples of Application		The New Zealand Advertising Standards Authority has processed and adjudicated on complaints arising from advertising on the internet. To enable implementation of a certification process separation from the Advertising Standards Authority is deemed preferable. The Ministry of Consumer Affairs is seeking effective mechanisms for consumer complaint resolution arising from internet purchases. It supports the establishment of eMSA as the mechanism for achieving this end.
Participation Public Sector		eMSA consulted with Government Agencies with the intent of obtaining governmental recognition and endorsement of a self regulatory regime for maintenance of standards for advertising on the internet.

Name of initiative		Online Ombuds Office
Objective		Online mediation and arbitration services
Enforcement mechanism(s)		
Leader(s) initiative	Issuing/ implementing organization(s)	Center for Information Technology and Dispute Resolution
	Supporting organization(s)	University of Massachusetts
[expected] Date of issuance / implementation		Established in 1996
Scope	General	Internet related disputes
	Sector	Commercial and Non-commercial
	Geographic	International and Domestic
Examples of application		Domain name disputes, consumer, intellectual property
Participation public sector		
For full text/further information consult/contact		www.ombuds.org , www.umass/dispute
Possible/expected evolution of the initiative		

Name of Initiative		Platform for Privacy Preferences (P3P)
Objective		Build privacy protection and personal information management tools into the infrastructure of the World Wide Web
Enforcement mechanism(s)		P3P is a voluntary technical specification
Leader(s) initiative	Issuing/ implementing organization(s)	World Wide Web Consortium
	Supporting organization(s)	330+ W3C member organizations around the world
[expected] Date of issuance / implementation		Fall 1999
Scope	General	Privacy protection
	Sector	
	Geographic	Global
Examples of application		Ecommerce services on the Web provide users information about site's privacy practices and give users control over handling of personal information according to the users individual preferences
Participation public sector		Active consultation with US Government, European Commission, and other national governments
For full text/further information consult/contact		Daniel J. Weitzner, Technology and Society Domain Leader, <djweitzner@w3.org> http://www.w3.org/p3p
Possible/expected evolution of the initiative		P3P may be the platform for empowering consumers to address consumer protection and choice of law issues in a global environment

Name of initiative		Paction – the model international sale contract application
Objective		Based on ICC's model contract for the international sale of goods, this new online service allows the parties to prepare, negotiate and complete contracts online.
Enforcement mechanism(s)		Once entered into, the contract is enforceable per usual means and the online application allows the parties to customize the contract to meet their specific needs.
Leader(s) initiative	Issuing/ implementing organization(s)	ICC (International Chamber of Commerce)
	Supporting organization(s)	
[expected] Date of issuance / implementation		Available now.
Scope	General	B2B
	Sector	Non sector-specific.
	Geographic	International
Examples of application		---
Participation public sector		None
For full text/further information consult/contact		http://www.modelcontracts.com Jonas ASTRUP +33-1-49532826
Possible/expected evolution of the initiative		---

Name of initiative		PKI Assessment Guidelines
Objective		<p>Describe the relevant components of a Public Key Infrastructure (PKI) and provide guidelines to assist certification authorities, relying parties, and other communities of interest, licensing or regulatory (including consumer protection) bodies, communities of interest, and others in making independent assessments of PKI trustworthiness. In particular, the PAG:</p> <ul style="list-style-type: none"> • provides a framework and guidelines for assessment of a PKI and PKI components, but does not mandate any particular criteria or conclusions; • explains the basics of PKI assessment covering such topics as relevant terminology, and a tutorial; • provides assistance in the drafting and analysis of certificate policies, certification practice statements; relying party agreements, and subscriber agreements, and • includes various useful annexes, including sample scenarios and corresponding considerations for "typical" trustworthy transactions that are intended to enhance interoperability and certainty. <p>The PAG is a logical extension of the Digital Signature Guidelines, (the "DSG"), a four and 1/2-year project of the American Bar Association's Information Security Committee published in August 1996. Although the focus and scope of the DSG and PAG differ, both are the product of intensive collaboration among technical, legal, business, and auditing professionals from around the world. Both are intended to facilitate secure electronic commerce.</p>
Enforcement mechanism(s)		Voluntary adoption
Leader(s) initiative	Issuing/ implementing organization(s)	Information Security Committee of the American Bar Association's Section of Science and Technology Law.
	Supporting organization(s)	Informal cooperation with diverse private and public entities.
Date of issuance / implementation		Public Draft for Comment published June 18 2001

Scope	General	Business-to-business as well as consumer-to-business also addresses government-to-citizen
	Sector	Non-sector specific
	Geographic	Global in scope
Examples of application		Quality assessment, evaluation for interoperability, underpinnings of seal programs, and basis for licensure.
Participation public sector		Considerable – informal and incremental participation in the ISC’s drafting of the PAG
For full text/further information consult/contact		www.abanet.org/scitech/ec/isc or contact Steve Wu and Kimberly Kiefer, Co-Chairs, Information Security Committee: swu@verisign.com and KKiefer@brobeck.com; Ben Wilson and Randy Sabett, Co-Vice Chairs, Information Security Committee, ben.wilson@trustdst.com and rsabett@cooley.com.
Possible/expected evolution of the initiative		Updated occasionally.

Name of initiative		Standard Contractual Clauses for Transborder Dataflows
Objective		Building on the widely supported 1992 ICC/EC/Council of Europe model clauses, as well as a Recommendation by the Council of the OECD, these model clauses are intended to bridge the gap that has widened between some jurisdictions as a result of different approaches to privacy protection and offer more flexible mechanism (compared to governmental contractual clauses) in transferring data across borders. Once approved by Data Protection Agencies (DPAs), they can be used as an alternative to the DPAs own standard contractual clauses in transferring personal data from the area under jurisdiction of the approving DPA.
Enforcement mechanism(s)		Once voluntarily incorporated into a contract, the clauses become fully enforceable on both of the contracting parties.
Leader(s) initiative	Issuing/ implementing organization(s)	International Chamber of Commerce (ICC), the Federation of European Direct Marketing (FEDMA), the EU Committee of the American Chamber of Commerce in Belgium (Amcham), the Japan Business Council in Europe (JBCE), the Confederation of British Industry (CBI), International Communications Round Table (ICRT), and the European Information and Communications Technology Industry Association (EICTA).
	Supporting organization(s)	
[expected] Date of issuance / implementation		Currently seeking approval from the European Commission
Scope	General	
	Sector	All sectors
	Geographic	All countries
Examples of application		Once approved by the European Commission, it can be used to ensure adequate protection for employee data being transferred from a subsidiary company in the EEA to a parent company outside the EEA.
Participation public sector		
For full text/further information consult/contact		http://www.iccwbo.org/home/statements_rules/statements/2001/itu.asp Ayesha Hassan, +33-1-4953013
Possible/expected evolution of the initiative		Will be updated as necessary

Name of initiative		TradeCard
Objective		To provide online transaction management and financial settlement for domestic and cross-border transactions that reduces the inefficiencies and uncertainties found in traditional domestic and cross-border trade transaction processes. To streamline and enhance the steps necessary for purchase order approvals, payment decisions and settlement, while providing a cost-effective, practical and patented service for financial supply chain management.
Enforcement mechanism(s)		Membership Contract ICC guidelines
Leader(s) initiative	Issuing/ implementing organization(s)	TradeCard Inc.
	Supporting organization(s)	
[expected] Date of issuance / implementation		First Quarter 2000
Scope	General	Business to business
	Sector	Import/Export Community
	Geographic	Global
Examples of application		Over 400 members conducting and settling transaction since November 1999. Members include some of the top U.S. retailers, electronics companies and apparel and footwear manufacturers. Also providing a white-labelled solution to banking institutions, i.e. JPMorgan Chase.
Participation public sector		
For full text/further information consult/contact		Michael Klausner, VP, Marketing mklausner@tradecard.com
Possible/expected evolution of the initiative		To reduce the barriers to trade To simplify and innovate the current trade finance process To increase the volume of world trade To reduce the cost of trade transactions

Name of Initiative		TRUSTe
Objective		Dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world"
Enforcement mechanism(s)		<p>Sites that choose to become licensees of the TRUSTe program must sign a one-year contractually binding licensing agreement. The agreement must be renewed each year. The agreement stipulates conditions by which the licensee must adhere, including privacy principles and escalation procedures. The site must demonstrate, to TRUSTe's satisfaction, compliance with the TRUSTe privacy principles prior to obtaining the TRUSTe seal or trustmark. Over the course of the contract, subsequent reviews are conducted by TRUSTe to ensure the site is in compliance with TRUSTe's privacy principles and their own stated privacy practices. A variety of mechanisms including offsite surfing of the site and "seeding" technologies are also used.</p> <p>The TRUSTe program also includes a consumer dispute resolution where consumers can voice concerns about TRUSTe licensees should their interactions with the licensee prove unsatisfactory. Complaints generated by either a consumer or TRUSTe follow a progressive escalation process that is dictated by the licensing agreement. Sites have agreed, by signing the contract, to cooperate with TRUSTe's review and appeals process. TRUSTe was approved by the U.S. Federal Trade Commission as a Safe Harbor for the Children's Online Privacy Protection Act in May 2001. It also offers a seal for Japanese Language Web sites, eHealth, EU safe</p>

		harbor, and Email Seal.
Leader(s) initiative	Issuing/ implementing organization(s)	TRUSTe—the digital industry’s only non-profit, self-regulatory effort focusing exclusively on individual privacy rights online.
	Supporting organization(s)	Founding Organizations: Electronic Frontier Foundation, CommerceNet Consortium
[expected] Date of issuance / implementation		Commercial launch of the program: June 1997
Scope	General	Business-to-consumer primarily, business-to-business secondarily
	Sector	All
	Geographic	US, with presence established in Europe and Asia
Examples of application		# of licensees: about 2000 sites as of January 2002 Influence of licensees: 15 of top 20 most visited sites, including all major Internet portals are TRUSTe licensees.
Participation public sector		TRUSTe has participated at a number of US government-sponsored forums including the FTC Privacy Workshops, the Department of Commerce Privacy Forum and privacy workshops. In addition, TRUSTe has testified at congressional hearings and has presented its program internationally to OECD-led privacy workshops.
For full text/further information consult/contact		www.truste.org Rebecca J. Richards rrichards@truste.org 1776 K St NW #360 Washington, DC 20006 1-202-483-1900 F: 1-202-719-7277
Possible/expected evolution of the initiative		The TRUSTe program has evolved in the 5 years since its commercial launch. It is anticipated that further developments and changes will occur as market and government forces dictate.

Name of initiative		TTP.NL
Objective		To stimulate the development of secure and trusted communication and storage of electronic information by developing a national, interoperable TTP-infrastructure which is in harmony with current market developments and needs. In the project TTP.NL working groups develop criteria that TTPs should comply with, an accreditation- and certification scheme and a supervising body that TTPs can join voluntarily.
Enforcement mechanism(s)		Accreditation- and certification scheme (to which TTP's can voluntarily adhere). Possibly a quality-mark for TTP's that participate.
Leader(s) initiative	Issuing/ implementing organization(s)	The Confederation of Netherlands Industry and Employers(VNO-NCW); the Dutch Ministries of Economic Affairs; Transport, Public Works & Water Management; the Dutch Electronic Commerce Platform (ECP.NL)
	Supporting organization(s)	Representatives of providers and users of TTP-services (a.o. notaries, post and banks), the Dutch private sector (a.o. consumer organizations, universities & large businesses).
[expected] Date of issuance / implementation		Summer 2002
Scope	General	Business-to-business; Business-to-consumer
	Sector	All sectors
	Geographic	
Examples of application		
Participation public sector		See "leaders initiative"

For full text/further information consult/contact	Marjolijn Bonthuis (marjolijn.bonthuis@ecp.nl) Marjolijn Durinck (marjolijn.durinck@ecp.nl)
Possible/expected evolution of the initiative	In the timeframe of the project, it is expected that the necessary infrastructure and "tools" for the development of TTP-services in the Netherlands should be completed. During the project all relevant market parties will be consulted and informed.

Name of Initiative		WebTrust
Objective		1) To build trust and confidence in eCommerce by increasing consumer confidence in using the Internet 2) Helping businesses deliver on their sales promises
Enforcement mechanism(s)		WebTrust involves a full-scope audit of a website by an independent, specially trained CPA, or their equivalents around the world, using the WebTrust Principles and Criteria as a benchmark to determine the soundness of on-line businesses' activities. Due to the nature of an audit, WebTrust is an effective eCommerce fraud deterrent and a comprehensive eCommerce seal of assurance. All WebTrust audits are performed on site and involve a critical review of online businesses internal control policies and procedures related to eCommerce.
Leader(s) initiative	Issuing/ implementing organization(s)	American Institute of Certified Public Accountants, Canadian Institute of Chartered Accountants
	Supporting organization(s)	
[expected] Date of issuance / implementation		Version 1.0 issued September 1997; Version 1.1 issued April 1999; Version 2.0 issued August 1999; Version 3.0 to be issued Summer 2002 under the umbrella concept of Information System Trust Services.
Scope	General	WebTrust entails an independent CPA performing an audit of a website's (1) business practices and privacy (tests to perform that an online business properly discloses business and privacy disclosures and can demonstrate compliance with those policies over a given time period); (2) transaction integrity (tests to determine that an on-line business can demonstrate a proven history of delivery goods and services at prices it agreed to with online consumers) (3) information security (tests to determine that appropriate security measures are in place (such as firewalls, SSL technology) both during transmission of data online and also once information reaches an on-line business and (4) confidentiality (tests focusing on confidential information obtained as a result of e-commerce from existing or potential business partners with an overall objective for the confidentiality of data exchanged over electronic networks such as the Internet or a Virtual Private Network..
	Sector	WebTrust is available to all sectors (public and private)
	Geographic	WebTrust is currently offered in the United States, Canada, the United Kingdom and Ireland, France, Australia, Argentina, Austria, Germany, Hong Kong, Italy, Netherlands, Scotland, Spain, and New Zealand. Plans are underway for future expansion into other European countries and Asia. Certain accounting firms have been granted world-wide licenses to offer WebTrust in any country where they have offices. WebTrust is scalable upwards to meet more rigorous laws or regulations in certain countries.
Examples of application		WebTrust is currently designed for use in business to consumer as well as a business to business applications. The AICPA has recently added WebTrust Confidentiality and WebTrust for Certificate Authorities applications.
Participation public sector		None
For full text/further information consult/contact		Anthony Pugliese, Director of Assurance Services (212) 596-6083, apugliese@aicpa.org Louis Matherne, Director and Assurance and Advisory Services, 212-596-6027

	Karyn Waller, Senior Technical Manager, Trust Services, (212) 596-6054, kwaller@aicpa.org
Possible/expected evolution of the initiative	The AICPA anticipates WebTrust will evolve into the recognized seal of choice by consumers and businesses alike due to the fundamental nature of the program itself. It represents an independent examination by a qualified CPA or their equivalents around the world. WebTrust is an effective self-regulatory model for government due to its inherent fraud detection capabilities and its comprehensive nature.

Name of initiative		World Chambers Network (WCN)
Objective		WCN allows chambers of commerce to promote their companies to the world and to network with other chambers of commerce around the world. Through their local chamber's participation, SME's have access to a global electronic network on the Internet for the exchange of business information and opportunities.
Enforcement mechanism(s)		Voluntary
Leader(s) initiative	Issuing/ implementing organization(s)	ICC (International Chamber of Commerce)
	Supporting organization(s)	ICC World Chambers Federation (WCF) Paris Chamber of Commerce and Industry G77 Chambers Trade Network
[expected]	Date of issuance / implementation	1994
Scope	General	Chamber-to-chamber. Business-to-business.
	Sector	Non sector-specific.
	Geographic	International
Examples of application		A manufacturer of personal conference phone found distributors in Mexico and Italy, and gained new US market information; Czech manufacturer of air fresheners found a buyer in Australia; joint venture in the production of bicycles was formed between a Czech bicycle company and a Macedonian firm. A company that sells ergonomic pens opened business contacts with one of the largest office supply chains in the United States. .
Participation public sector		None
For full text/further information consult/contact		http://www.worldchambers.com Anthony Parkes, +33-1-49532967
Possible/expected evolution of the initiative		WCN will link into its system, the products and services of the chambers of commerce around the world. The network will expand its qualified, validated business opportunity service, providing a higher level of trust through the intervention of trusted third parties - chambers of commerce.

About the Alliance for Global Business

The Alliance for Global Business (AGB, “the Alliance”) is a coordinating mechanism of leading international business organizations created to provide private sector leadership on information society issues and electronic commerce. Jointly, these organizations represent the bulk of electronic commerce in almost all countries in the world. The coalition represents a diverse cross section of business in over 140 countries. Membership includes providers and users of information technology, large multinational enterprises and small start-ups, and companies in developing as well as developed economies.

The AGB's founding members are:

BIAC – Business and Industry Advisory Committee to the OECD

www.biac.org

The Business and Industry Advisory Committee to the OECD (BIAC) is the voice of business from the economically advanced democratic nations of the world. Recognized by the OECD since 1962 as its business advisory counterpart, BIAC has the mission of ensuring that the OECD hears a broad-based, considered business advice on all sectors of activity that it embarks upon. BIAC's membership consists of the principal industrial and employers' organizations of the OECD Member countries. These represent the majority in terms of employment, output, assets and investment by the private sector in the advanced market economies. Over the years BIAC, its member organizations, and their member companies have been deeply involved in the work of OECD on information and communications and electronic commerce, through direct participation in OECD committees as observer and by providing technical and policy advice to various processes that develop OECD instruments such as the 1980 “Privacy Guidelines”, the 1997 Cryptography Guidelines or more recent work on Information security.

GIIC - Global Information Infrastructure Commission

www.giic.org

The Global Information Infrastructure Commission (GIIC) is a confederation of chief executive officers of business firms that develop and deploy, operate, rely upon, and finance information and communications technology infrastructure facilities. Together as GIIC commissioners, these executives are dedicated to providing private sector leadership to speed the spread of information infrastructure throughout the world. The GIIC was established during a 1995 Group of Seven (G7) meeting in Brussels at which the political heads of the world's leading national economies formally and for the first time acknowledged the transforming forces of computer and telecommunications technologies, i.e., the emergence of an “information society”. In doing so, the heads of state challenged business leaders to unite in the promotion of public policies and information technology applications likely to spur needed private sector investment in public communications infrastructure facilities. Commissioners of the GIIC come from developed nations, emerging markets, and less developed countries. The GIIC carries out its work in a variety of ways: by preparing and disseminating papers on public policy topics and promising information and communications technology applications (most particularly e-commerce); publishing a quarterly journal;

conducting outreach programs throughout the world; disseminating e-mail advisories; sponsoring meetings; informally meeting with representatives of national government communications ministries; and collaborating with other organizations. If there is a hallmark event on the GIIC calendar it is the organization's annual forum. Each year the site of the forum shifts from the Americas, Europe-Africa, and Asia-Pacific regions.

ICC - International Chamber of Commerce

www.iccwbo.org

ICC is the world business organization. With corporate and business organization membership in more than 130 countries, it is the only representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world. Founded in 1919, ICC's purpose is to promote an open international trade and investment system and the market economy worldwide. Its rules for international trade transactions and trade finance are accepted globally by traders, governments and judges. The ICC International Court of Arbitration is the world's leading institution of its kind. ICC brings together executives and experts from all sectors of business to establish the business stance on broad issues of trade and investment policy as well as on vital technical or legal subjects. ICC's broad framework of rules for international trade and commerce evolves continuously to take into account changes in business practice. ICC has issued best practice rules for electronic business since the 1980s and continues to harmonize business rules and practices to meet the needs of the networked economy.

ICC's Commission on E-Business, I.T. and Telecoms is made up of business leaders and experts drawn from the ICC membership of companies of all sizes in more than 35 countries. This Commission establishes key business positions, policies and practices, creates rules and tools for trustworthy electronic business, and an industry interface with all the relevant intergovernmental organizations.

INTUG - International Telecommunication Users Group

www.intug.int

INTUG is an international association of users of communications technology and applications. It has an extremely wide constituency. Founded in 1974, it has its Secretariat in Brussels where it is registered as an international non-profit organization. It meets in plenary session four times a year. Members include national users groups which represent the interests of users in Europe, the Americas, Asia-Pacific and Africa. Associate and individual members come from major multinational enterprises, academia, law and other relevant industry sectors. Many of INTUG's member groups have been particularly successful in their interaction with national government policy makers; also in regional economic policy forums. INTUG itself promotes the interests of all users at the international level and ensures that the voice of the user is clearly heard whenever communications policy issues are addressed. Its Special Interest Group on Y2K issues has been extremely active and was a specific focus of the INTUG meeting in Brussels in June 1998.

WITSA - World Information Technology and Services Alliance

www.witsa.org

The World Information Technology and Services Alliance (WITSA) is a consortium of The World Information Technology and Services Alliance is a consortium of 46 information technology (IT) industry associations from economies around the world. As the global voice of the IT industry, WITSA is dedicated to advocating policies that advance the industry's growth and development; facilitating international trade and investment in IT products and services; strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information; providing members with a vast network of contacts in nearly every geographic region of the world; and hosting the World Congress on IT, the only industry sponsored global IT event. Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure

The WITSA Secretariat is currently hosted by the Information Technology Association of America (ITAA). For more information about ITAA, please visit its web site at <http://www.ita.org>.

© 2002

Business and Industry Advisory Committee to the OECD (BIAC)

Global Information Infrastructure Commission (GIIC)

International Chamber of Commerce (ICC)

International Telecommunication Users Group (INTUG)

World Information Technology and Services Alliance (WITSA)

All rights reserved.