International Chamber of Commerce
The world business organization

An ICC initiative
BASIS
Business Action to Support the Information Society

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

ICC compendium of Internet governance related policy and practice tools

Presented at the Internet Governance Forum (IGF) Athens, 2006

October 2006

Foreword

We are pleased to present this selection of policy and practice documents prepared by ICC's Commission on E-Business, IT and Telecoms at the first Internet Governance Forum (IGF), in Athens Greece. The selection has been prepared specifically for the IGF in Athens with the main topics of Openness, Security, Diversity, Access, and the cross-cutting theme of capacity building in mind. It gives a comprehensive picture of the substantive work of ICC's experts on the public policy aspects of these Internet governance issues.

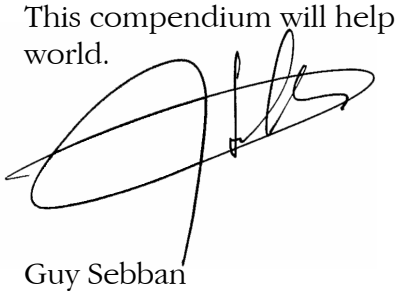
As ICC and its new Business Action to Support the Information Society initiative, BASIS, provide a global focal point for business around the world, it is well placed to contribute substantive resources to help raise awareness about best practices that are available to all stakeholders and key policy positions to be considered as frameworks are put in place to ensure that the Internet and ICT infrastructures can be used by more people around the world. Although by no means exhaustive, the compendium presents ICC member expertise and business experience in over 130 countries from all business sectors and companies of all sizes. It provides a truly global business perspective on many of the issues that will be discussed at the IGF.

The policy recommendations are based on extensive consultation among business experts. ICC policy documents undergo rigorous vetting by ICC national committees and members in over 130 countries and reflect a wide range of business opinion and expertise .

ICC recognizes that having the right policy framework in place is an essential but not sufficient condition for the Internet, ICTs and e-business to thrive. We complement our policy work by providing the practical means for businesses to constantly improve their operations. From online best practice guides to model contract clauses and ICC's many trade tools, our organization strives to give businesses and users what they need to develop and grow.

We invite participants in the Internet Governance Forum to take this comprehensive collection of global business expertise home to their own countries and start putting the recommendations into practice. We hope that participants find this useful. It is also available electronically on the IGF website http://www.intgovforum.org/ and the ICC/BASIS website at http://www.iccwbo.org/basis/id8215/index.html

This compendium will help governments, business, consumers and users around the world.



Guy Sebban
ICC Secretary General

Talal Abu-Ghazaleh
Chair, ICC Commission on
E-Business, IT and Telecoms (EBITT)
Chair, Business Action to Support the
Information Society (BASIS)

How to use this compendium

The documents in this compendium are meant to inform and assist decision-makers, business and other stakeholders worldwide in formulating policies relating to the use and development of the Internet and ICTs. You are encouraged to use these positions, business tools and information in your country and to disseminate them widely, while attributing them to ICC. If you would like more information, please contact the ICC International Secretariat using the contact details below.

Further information and other ICC work products are available on the ICC website: http://www.iccwbo.org/home/menu_electronic_business.asp

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

Ayesha Hassan
Senior Policy Manager
Tel: +33 1 49 53 30 13
Fax: +33 1 49 53 28 59
Email: aha@iccwbo.org

Manuela van der Laan
Policy Manager
Tel: +33 1 49 53 28 07
Fax: +33 1 49 53 28 59
Email: mvdl@iccwbo.org

Contents

Section 1
Revised and updated matrix of issues related to the Internet and organizations dealing with them *(2 May 2006)*

Section 2
ICC policy statement on "spam" and unsolicited commercial electronic messages *(2 December 2004)*

Section 3
Policy Statement focused on European Union Context Employee privacy, data protection and human resources *(4 December 2003)*

Section 4
Final Approved Version of Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries (controller to controller transfers)

Section 5
Issues Paper on Internationalized Domain Names *(7 July 2006)*

Section 6
Policy Statement The impact of Internet Content regulation (*18 November 2002*)

Section 7
Policy Statement ICC Framework for consultation and drafting of Information Compliance obligations *(15 June 2006)*

Section 8
Policy Statement Open Source Software *(27 October 2005)*

Section 9
Deploying the next generation Internet: ICC Statement on the introduction of IPv6 *(2 December 2004)*

Section 10
Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data outside the EU *(5 July 2006)*

Section 11
ICC Tools for E Business

Section 1
Revised and updated matrix of issues related to the Internet and organizations dealing with them *(2 May 2006)*

International Chamber of Commerce
The world business organization

Department of Policy and Business Practices

Commission on E-Business, IT and Telecoms

Task Force on the Internet and IT Services

Revised and updated matrix of issues related to the Internet and organizations dealing with them[1]

2 May 2006

Introductory note:

This matrix is meant to identify issues related to the Internet generally and the government, intergovernmental, international, multistakeholder, private-sector and business actions and initiatives that are currently addressing or discussing them. It has been revised to assist in the discussions related to 'Internet governance' and the Internet Governance Forum (IGF)[2], what issues are being addressed and where, and whether there are any issues that are not being addressed.

While this matrix has been developed for the Internet and organizations dealing with it, similar charts could be constructed for other broad information and communications network topics, e.g. the public switched telephone network (PSTN), to reflect issues such as these and the organizations addressing each issue.

Business does not view all of these issues to necessarily be part of 'Internet governance' but rather all of the issues set forth below are related to the Internet.

[1] This matrix is the newly updated version of the 13 September 2004 ICC matrix on these issues.
[2] Internet Governance Forum Website www.intgovforum.org

International Chamber of Commerce
38, Cours Albert 1er, 75008 Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Website www.iccwbo.org E-mail icc@iccwbo.org

Issue	National government actions and initiatives [3],[4]	Intergovernmental organization actions and initiatives [5]	Private sector and business actions and initiatives [6]
Capacity Building/E-skills Education	National aid programs Local infrastructure initiatives (e.g. city-wide wi-fi networks) "Digital Literacy" education and training initiatives	2005 WSIS "Tunis Agenda for the Information Society" Statement UN ICT Task Force GeSCi initiative The European Union "i2010" initiative ITU-D conference for development of digital infrastructure (Doha action plan), March 2006 ITU "Connect the World" global multistakeholder initiative G8 DOT Force Initiative Recommendations	Corporate "hybrid initiatives" combining philanthropy and direct investment Business support for telecommunications accessibility approach Private corporate investment initiatives (e.g. HP e-inclusion project, Cisco Networking Academy Programme) Computer Technology Industry Association (CompTIA) initiatives for IT skills development

[3] National public policy matters are, in general, the responsibility of governments in terms of decision-making. However, policy discussions and development must include the active participation of business and other stakeholders.

[4] In many cases, general national policies are applicable and no sector specific or ICT-specific policies are required.

[5] In many cases, general international guidelines or agreements are applicable and no sector specific or ICT-specific policies are required.

[6] Private Sector is broadly defined to include non-governmental stakeholders, though the bulk of listed activities are business related. We look forward to working with other stakeholders to expand this section of the matrix to include their activities. Business actions and initiatives are informed by the policies of the nation in which they are achieved. In many cases, these actions and initiatives are in partnership with governments, civil society and international organizations.

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Consumer protection	Education and awareness raising programmes National policy regime options: 1. Regulation and legislation 2. Self-regulatory initiatives National, regional and local law enforcement cooperation	2000 OECD Guidelines for Consumer Protection in the Context of E-commerce 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders APEC Voluntary Consumer Protection Guidelines for the Online Environment Bilateral and multilateral government law enforcement and cooperation internationally	Education and awareness raising programmes Self-regulatory codes and enforcement organizations (e.g. BBBOnline) Provision of alternative dispute resolution services Development and dissemination of industry best practices (e.g. ICC Tools for E-Business: "Putting it right: Best practices for customer redress in online business", "Resolving disputes online: Best practices for online dispute resolution in B2C and C2C transactions"; and GBDe policies on consumer confidence and legal (jurisdiction) aspects)
Content	National legislation on access to or the dissemination of certain content	OECD Workshop on Online Content European Union "Safer Internet Programme"	Self-regulatory schemes (e.g. Internet Content Rating Association, filtering technologies) Innovation and development of content filtering tools for use by parents, service providers, etc.
Contractual issues	Legislative measures to ensure legal validity and recognition of electronic contracts	UNCITRAL Model Law on Electronic Commerce UNCITRAL Draft convention on electronic contracting	Provision of alternative dispute resolution services. ICC E-Terms 2004 electronic contracting tools ICC Guide to e-contracting

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Cryptography	National policies related to cryptography	Wassenaar Arrangement on the export of dual-use goods including encryption products OECD Guidelines on Cryptography Technical standards in the ITU (also see below under Technical Standards)	Technical standards in the IETF, W3C, IEEE, ISO/IEC, etc. (also see below under Technical Standards) Innovation and deployment of cryptographic technologies
Customs duties on electronic transmissions	The assessment of Customs duties on electronic transmissions	WTO moratorium on customs duties on electronic transmissions	Cooperation with customs and other entities considering this issue Business support of the WTO moratorium on customs duties on electronic transmissions
Cyber-crimes	National legislation and regulation making certain online acts criminal	Council of Europe Convention on Cyber-crime (Note: non-members can accede to the Convention upon application and approval)	Cooperation with law enforcement ICC commercial crime services (CCS) Fraudnet initiative
Education	National, regional, and local educational systems from basic education to university, to IT specific training	UNESCO UNICT TF Forums/Workshops ITU and UNDP Human Capacity Building programs in IT	Numerous private sector capacity building exercises and public-private partnerships (e.g. Cisco network academies, Microsoft, Cable and Wireless Virtual Academy, Nokia BridgeIT programme) Internal corporate training and life-long learning programmes

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Electronic Authentication	Encouragement of use by business and the public of electronic authentication in e-government, (e.g. in tax filing, and government procurement) Legislative measures to ensure legal validity and recognition of electronic signatures	OECD Ministerial Declaration on electronic authentication OECD-Private Sector workshop on electronic authentication UNCITRAL Model Law on Electronic Signatures European Electronic Signature Standardisation Initiative (EESSI) Technical standards in the ITU on public key infrastructure (also see below under Technical Standards)	Development and dissemination of guidance on electronic authentication (e.g. ICC General Usage for International Digitally Ensured Commerce (GUIDEC)) GBDe recommendations on authentication Innovation and deployment of electronic authentication technologies
Exchange of Internet Traffic	Ensure that there are no legal barriers to the creation of regional traffic hubs Competition Law	ITU Recommendation D.50 ITU-T Rapporteurs Group continues to discuss this issue OECD Workshop "Internet Traffic Exchange" OECD Study "Internet Traffic Exchange and the Development of End-to-End International Telecommunication Competition" ITU assistance in establishing regional Internet Exchange Points APECTEL Working Group	Commercial negotiations among ISPs to exchange traffic (e.g. peering and transit) Business investment in infrastructure including establishing Internet Exchange Points

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Freedom of expression/Human rights	Legislative and judicial measures protecting freedom of expression on the internet (e.g. U.S. Supreme Court ruling protecting the Internet under the 1st amendment)	Joint Declaration by UN/OSCE/OAS on Freedom of Expression on the Internet Joint recommendation by OSCE and Reporters sans Frontières to ensure freedom of expression on the internet United Nations Universal Declaration on Human Rights Article 19 Council of Europe human rights media division UNESCO Freedom of expression in cyberspace conference	Private sector digital rights advocacy associations (e.g. Electronic Frontier Foundation (EFF), Center for Democracy and Technology (CDI), Reporters sans Frontières (RSF)) Statement by private investment funds in conjunction with Reporters sans Frontières for freedom of expression on the internet WSIS Civil Society and Human Rights Caucus statement to IGF open consultations

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Information systems and network security	Education and awareness raising programmes, development and dissemination of best practices (e.g. FCC industry advisory group Physical and Cybersecurity Best Practices (voluntary)) Training and recruiting of technical specialists for law enforcement Dedicated information security incident reporting to law enforcement (e.g. UK National Hi-Tech Crime Unit) Support/encourage incident-reporting and information-sharing centres in the private sector Legislation on computer-related crime	Coordination and information-sharing of national initiatives/centres on systems and network security (e.g. European Network and Information Security Agency) 2002 OECD Guidelines on the Security of Information Systems and Networks (revised 2003) UN General Assembly Resolution on a Global Culture of Security APEC TEL 2005 Strategy to ensure trusted, secure and sustainable online environment OAS' CITEL PCC.I Working Group on Advanced Technologies and Services Technical standards in the ITU-T (see below under Technical Standards) ITU-D programs on e-strategies /applications to enhance security and trust in the use of networks	Incident reporting and information-sharing resources (e.g. National Computer Emergency Response Team for Australia, CERT® Coordination Center, US, ICC Commercial Crime Services, UK) Education and awareness raising, development and dissemination of best practices for industry and the general public. (e.g. national reporting and information sharing groups; ICC/BIAC business applications of OECD security guidelines, "Securing Your Business", WITSA Statement on Information Security) Technical standards in the IETF, W3C, IEEE, ISO/IEC, etc. (see below under Technical Standards) ICC Toolkits: "Information Security Assistance for Executives" and "Securing Your Business: Information security issues and resources for small and entrepreneurial companies" GBDe recommendations on security Innovation and deployment of information systems and network security technologies

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Infrastructure development	National economic development programs Incentives to private investment, e.g. "good governance" National Universal Service obligations for basic telecommunications	WTO Information Technology Agreement (ITA) and Global Procurement Agreement (GPA), Relevant Services Commitments, e.g. Telecoms, Computer and Related Services World Bank UNESCO's ICT development programs UNCTAD ICT and E-Business Branch UNDP's ICT development programmes	Advocacy and best practice work on trade liberalization in telecommunications (e.g. ICC Business Guide to Telecoms Liberalization, WITSA paper "Best Practices in IT Government Procurement") Private sector investment and deployment of infrastructure
Intellectual Property	Implementation of national policies and enforcement of national laws and international agreements	World Intellectual Property Organization (WIPO) Copyright Treaty (WCT), 1996 World Intellectual Property Organization (WIPO) Performances and Phonograms Treaty (WPPT), 1996 WIPO Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet, 2001 WTO Agreement on the Trade Related Aspects of Intellectual Property (TRIPS)	Innovation and deployment of digital rights management technologies ICANN Uniform domain-name dispute resolution policy (UDRP) ICC Intellectual Property (IP) roadmap Education and awareness raising programmes Enforcement of rights

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
IPv6 Deployment	National Government Initiatives for promotion of IPv6 Deployment of IPv6 in government applications	European Commission IPv6 Task Force IPv6 Forum North American IPv6 Task Force IPv6 Cluster European IPv6 Internet portal 6DISS European initiative for dissemination and exploitation of IPv6 in developing regions Euro6IX Research IPv6 research program	IETF IPv6 working group ICC Policy Statement on IPv6 "Deploying the next generation Internet" Open Contributors Corporation for Advanced Internet Development (OCCAID) Private IPv6 Research and Promotional Consortia (e.g. WIDE Japan, IPv6 Promotion Council Japan, 6Bone) National Level IPv6 Alliances and Promotional Groups (e.g. IPv6 France Task Force, China IPv6 Council, IPv6 Forum Taiwan, IPv6 Forum Korea)
Multilingual (internationalized) Domain Names (IDNs)	National acceptance of international standards	ITU and UNESCO Global Symposium on Promoting the Multilingual Internet Geneva, 9-11 May 2006 ITU Specific activities: Internationalized Domain Names (IDN) Joint ITU/WIPO symposium, Geneva 2001	Internet Corporation for Assigned Names and Numbers (ICANN), including coordination with root servers, IANA Internet Engineering Task Force (IETF), including technical and linguistic (IDNA) standards Multilingual Internet Names Consortium (MINC), including language tables ICC Issues paper on Internationalized Domain Names The Unicode Consortium including the Unicode Standard character database

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Privacy and cross-border flows of personal data	National privacy regime options: 1. General and/or sectoral regulation 2. Omnibus and sectoral legislation 3. Self-regulatory initiatives Education and awareness raising activities	OECD Guidelines for the protection of privacy and transborder flows of personal data OECD Privacy Online: policy and practical guidance OECD Privacy policy statement generator OECD work on Spam UN Guidelines for the regulation of computerized personal data files Council of Europe Convention European Commission Directive 95/46/EC APEC Privacy Framework	Education and awareness raising (e.g. ICC Global Spam Fighting Resource, ICC Privacy Toolkit) Self-regulatory codes and enforcement organizations (e.g. ICC Guidelines on Marketing and Advertising on the Internet, Truste, BBBOnline) ICC policy paper on Spam Provision of reporting and 'optout' services. (e.g. national direct marketing associations) Company codes of conduct / binding corporate rules Model contract clauses for cross-border transfers of personal data including the industry alternative model contract clauses for data transfers from the EU GBDe recommendations for protection of personal data Innovation of new technologies to protect information, mitigate SPAM, etc.
Taxation of e-commerce	National policies regarding the taxation of electronic commerce	OECD Technical Advisory Group's recommendations on current taxation treaties	Work of the OECD Technical Advisory Groups on Tax in partnership with business

Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
Technical coordination of the Internet	National laws apply to ccTLD administrators	Governmental Advisory Committee (GAC) to ICANN and ITU activities under Resolution 102 (Marrakech 2002) GAC guidelines for the delegation and administration of country code top level domains (ccTLD)	Internet Corporation for Assigned Names and Numbers (ICANN) The Internet Assigned Numbers Authority (IANA) Organizations such as CENTR, RIPE-NCC, APNIC etc.
Technical standards	Support for and participation in national standards setting bodies/processes Participation in international standards setting bodies	United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) ITU-T and ITU-R Recommendations for the telecommunications network and radio ITU-R (WRC) identification, allocation and assignment of radio spectrum ITU-R (global regulations for frequency allocations)	Organizations involved in interface and performance standardization, including protocols: Internet Engineering Task Force (IETF), the Internet Engineering Steering Group (IESG) and the Internet Architecture Board (IAB) World Wide Web Consortium (W3C) Institute for Electrical and Electronic Engineers (IEEE) International Organization for Standards (ISO) International Electrotechnic Commission (IEC) Session Initiation Protocol (SIP) Forum

Glossary

American Civil Liberties Union	ACLU	www.aclu.org
APEC Telecommunication and Information Working Group	APEC TEL WG	www.apectelwg.org
Asia Pacific Network Information Centre	APNIC	www.apnic.net
Asia-Pacific Economic Cooperation	APEC	www.apec.org
Better Business Bureau OnLine, Inc.	BBBOnLine	www.bbbonline.org
Business and Industry Advisory Committee to the OECD	BIAC	www.biac.org
Center for Democracy and Technology	CDT	www.cdt.org
CERT® Coordination Center	CERT/CC	www.cert.org
Cisco Academies		www.cisco.com/web/learning/netacad/index.html
Computing Technology Industry Association	CompTIA	www.comptia.org
Council of Europe	CoE	www.coe.int
Council of European National Top-Level Domain Registries	CENTR	www.centr.org
Electronic Frontier Foundation	EFF	www.eff.org
European Commission IPv6 Task Force		www.ec.ipv6tf.org/in/i-index.php
European IPv6 Internet Exchanges Backbone	Euro6IX	www.euro6ix.org/main/index.php
Federal Communications Commission	FCC	www.fcc.gov
Global Business Dialogue on Electronic Commerce	GBDe	www.gbde.org
Governmental Advisory Committee to ICANN	GAC	www.gacsecretariat.org
Hewlett-Packard E-inclusion Program		www.hp.com/e-inclusion/en/index.html
ICC Commercial Crime Services	CCS	www.iccwbo.org/index_ccs.asp
Institute of Electrical and Electronics Engineers, Inc	IEEE	www.ieee.org
International Chamber of Commerce	ICC	www.iccwbo.org
International Electrotechnical Commission	IEC	www.iec.ch
International Organization for Standards	ISO	www.iso.org
Internet Architecture Board	IAB	www.iab.org
Internet Assigned Numbers Authority	IANA	www.iana.org
Internet Content Rating Association	ICRA	www.icra.org
Internet Corporation for Assigned Names and Numbers	ICANN	www.icann.org
Internet Engineering Steering Group	IESG	www.ietf.org/iesg.html
Internet Engineering Task Force	IETF	www.ietf.org
Internet Governance Forum	IGF	www.intgovforum.org
Internet Society	ISOC	www.isoc.org
IPv6 Dissemination and Exploitation	6DISS	www.6diss.org
IPv6 Forum		www.ipv6forum.com/
IPv6 Portal		www.ipv6tf.org/
ITU Radiocommunication Sector	ITU-R	www.itu.int/ITU-R/
ITU Telecommunication Development Bureau	ITU-D	www.itu.int/ITU-D/
ITU Telecommunication Standardization Sector	ITU-T	www.itu.int/ITU-T/
Multilingual Internet Names Consortium	MINC	www.minc.org

National Computer Emergency Response Team for Australia	AusCERT	www.auscert.org.au
National Hi-Tech Crime Unit	NHTCU	www.nhtcu.org
North American IPv6 Task Force	NAv6TF	www.nav6tf.org/
Organisation for Economic Co-operation and Development	OECD	www.oecd.org
Organization for Security and Co-operation in Europe	OSCE	www.osce.org
Organization of American States' Inter-American Telecommunication Commission (CITEL) Permanent Consultative Committee I (Public Telecommunications Services)	OAS' CITEL PCC I	www.oas.org/en/oas/citel.htm
Reporters Sans Frontières	RSF	www.rsf.org (English)
RIPE (Réseaux IP Européens) Network Coordination Centre	RIPE NCC	www.ripe.net
Session Initiation Protocol Forum	SIP Forum	www.sipforum.org
United Nations	UN	www.un.int
United Nations Commission on International Trade Law	UNICTRAL	www.uncitral.org
United Nations Conference on Trade and Development	UNCTAD	www.unctad.org
United Nations Development Programme – Sustainable Development Networking Programme	UNDP	www.sdnp.undp.org
United Nations Educational, Scientific and Cultural Organization – Communication and Information Sector	UNESCO	www.unesco.org/webworld/index.shtml
United Nations Information and Communication Technologies Task Force	UN ICT Task Force	www.unicttaskforce.org
World Bank		www.worldbank.org
World Intellectual Property Organization	WIPO	www.wipo.int
World Information Technology and Services Alliance	WITSA	www.witsa.org
World Trade Organization	WTO	www.wto.org
World Wide Web Consortium	W3C	www.w3c.org

The International Chamber of Commerce

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

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

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

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

Within a year of the creation of the United Nations, ICC was granted consultative status at the highest level with the UN and its specialized agencies.

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

ICC was founded in 1919. Today it groups thousands of member companies and associations from over 130 countries. National committees work with their members to address the concerns of business in their countries and convey to their governments the business views formulated by ICC.

International Chamber of Commerce

The world business organization

38, Cours Albert 1er, 75008 Paris, France

Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59

Web site www.iccwbo.org E-mail icc@iccwbo.org

Section 2
ICC policy statement on "spam" and unsolicited commercial electronic messages *(2 December 2004)*

Policy Statement

ICC policy statement on 'spam'[1] and unsolicited commercial electronic messages

Prepared by the Commission on E-Business, IT and Telecoms

Introduction

Businesses and consumers around the world have come to rely on the speed and convenience of e-mail and other types of electronic communications. In the space of a few short years e-mail has become an essential tool to do business, get information, and keep in touch. There has been much controversy about the problem of "spam" and how it may be curtailed. As different legal rules apply to electronic communications in different jurisdictions, there is no generally accepted definition of the term 'spam.' Consequently, our purpose in this paper is to identify illegitimate or unacceptable electronic communications, a topic on which we believe there is general agreement.

> By 'spam', ICC means harmful, fraudulent, malicious, misleading or illegal communications, generally sent in bulk. This is the definition of 'spam' as used in this paper.
>
> By 'spammers', we mean entities sending 'spam' as defined above.
>
> The section below focuses on describing unacceptable electronic messages and differentiating them from acceptable electronic commercial marketing messages that follow accepted codes of industry practice.

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

- It recognizes the legitimate needs and benefits of commercial electronic communications, and
- It allows governments and others to focus on the real problem of harmful, fraudulent, malicious, misleading or illegal communications.

[1] The term 'spam' is used in this document because it is currently the commonly used term

38, Cours Albert 1er, 75008 Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Web site www.iccwbo.org E-mail icc@iccwbo.org

1. Responsible and legitimate marketing practices are the basis of self-regulation

ICC supports a coherent self-regulatory framework in which all parties in marketing and advertising share their proportionate responsibility for marketing messages sent using electronic media. This means that companies should follow industry codes that set standards of ethical conduct, such as the ICC Guidelines on Marketing and Advertising Using Electronic Media, revised and updated in 2004.

Responsible and legitimate marketers who follow the ICC relevant[2] guidelines will take measures including the following:

- When collecting personal data, follow the provisions in the ICC International Code on Direct Marketing[3] on informing the data subject, collection, use and transfer of data, security of data and provision and use of privacy policy statements. In jurisdictions where no privacy legislation currently exists, companies should consider observing the privacy principles outlined in the ICC Privacy Toolkit.[4]

- Target messages so that their recipients are likely to have an interest in the subject matter or offer.

- Do not use misleading subject headers in commercial emails.

- Disclose the identity and contact details of the sender, allowing recipients to opt out of future marketing messages.

Companies that follow these guidelines are clearly different from entities sending spam. To focus government efforts where they are most needed and to ensure the communications networks continue to be a viable means of commercial communication for legitimate businesses, it is essential for public policy to recognize this difference. We strongly encourage governments to focus their efforts on measures that will target without penalizing legitimate marketers.

2. Legitimate marketing-focused electronic communications are not 'spam'

The fact that an electronic communication has a commercial nature in and of itself does not make that communication 'spam'. Spam - harmful, fraudulent, malicious, misleading or illegal communications, generally sent in bulk – often has the following characteristics:

- It may include false header information or an opt-out mechanism that does not work or is not honoured; i.e. it may be fraudulent and misleading.

- It may be used to advertise products and services with misleading claims, or sell products such as prescription drugs illegally; i.e. it may be misleading, illegitimate and potentially harmful.

- Spammers may acquire individuals' contact details in unethical, illegal, or misleading ways;

[2] The ICC International Code on Direct Marketing includes provisions on the collection of personal data.
[3] Available online at http://www.iccwbo.org/home/statements_rules/rules/2001/code_of_direct_marketing.asp
[4] Available online at http://www.iccwbo.org/home/e_business/word_documents/TOOLKIT-rev.pdf

i.e. it may be illegitimate/illegal.

- As described below, spam may be the vehicle for viruses or fraudulent schemes; i.e. it may be malicious and illegal.

Put simply, the entities that send spam differ from legitimate marketers because spammers do not respect applicable laws and regulations and do not honour users' preferences regarding commercial communications. This is the essence of spam.

3. Not all 'spam' messages have a commercial intent.

An increasing proportion of spam messages – particularly emails – have no marketing or solicitation purpose at all, and are sent primarily to spread computer viruses (e.g. the ILOVEYOU virus) or as a means to fraudulently acquire personal information. The latter type of message, known as 'phishing', may purport to be from a legitimate business or bank, and ask for individuals' credit card numbers, bank account details or other personal information. These messages may even include links to bogus or 'spoofed' websites that lure users into providing their personal information. Once acquired, the personal information can be used to commit identity theft and de-fraud individuals and organizations. This is becoming a serious information security issue giving a new aspect to the problem of spam.

In their frustration over harmful or fraudulent electronic messages, some countries have banned all unsolicited commercial communications. However, these measures have not shown any appreciable decrease in the volume of spam because senders of spam operate outside the law, respecting neither 'opt-in' nor 'opt-out' rules. Not only has the real problem worsened, but marketing by email has been made much more cumbersome and costly to legitimate businesses. 'Opt in' measures have lessened the ability of legitimate businesses, particularly small and medium businesses, to maintain and expand their customer bases using the responsible, targeted use of innovative marketing techniques made possible by the Internet.

The toolkit approach to fighting spam

Spam – harmful, fraudulent, misleading or illegal messages generally sent in bulk, and not simply "unsolicited" or unauthorized electronic messages - is a serious, international, cross-sectoral problem that must urgently be tackled by the coordinated efforts of all interested parties in the information society. It harms consumers and business, as both are users of information and communication technologies. Dialogue and exchange of expertise between the public and private sectors are vital to successfully address this challenge, and to ensure that the networked economy continues to benefit users worldwide.

The private sector brings unique and valuable insights to this dialogue. As business owns and manages many of the networks and systems that are most burdened with spam, the business community has significant and up to date expertise in fighting spam. Most importantly, business plays a fundamental role in developing the innovative technological solutions that address spam. We look forward to continued and constructive dialogue, at all levels and with all affected stakeholders, to foster workable and effective solutions to spam.

Business endorses a multi-faceted approach to fighting spam:

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

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

1. Education and co-operation: Business and government must work together in public-private partnership to educate users and businesses in the fight against spam.

Effective awareness and education is the primary tool in combating spam as it provides users with important tools they need to manage their e-mail and personal information. As users learn to reduce and deal effectively with spam, it will become a less attractive activity for spammers. Users need to be discerning when releasing their e-mail addresses and how to use software and other tools to deal with spam addressed to them.

Awareness and education are the joint responsibility of all stakeholders. Industry continues to inform users about how to protect the privacy of their information when registering with a website or purchasing a product. Industry also exchanges information on best practices for effective spam-handling procedures, and develops tools that empower users to choose which e-mail they will receive. As industry is at the cutting edge of dealing with spammers' latest techniques, it is best positioned to understand the problem and to introduce solutions. Industry will work with relevant stakeholders to promote awareness among users and to disseminate new and more effective methods to avoid or reduce spam.

- Governments should support and complement industry efforts to educate users (including SMEs) on avoiding and reducing spam, and managing their personal information online.
- Governments should work with industry to increase awareness and use of workable solutions and mechanisms to report and deal with e-mail, instant messaging or SMS abuse. Governments and business should input reporting and opt-out web addresses to the ICC

Global Online Resource on Spam,[5] an online resource for users to report spam and make privacy complaints, with links to reporting and opt-out resources in over thirty countries around the world.

- Business should continue and expand efforts to make more businesses aware of acceptable marketing practices by educating them about encouraging them to become compliant with self-regulatory codes.

2. Technology: Industry should continue to develop technological solutions to spam, working with governments and consumers to promote awareness of technological approaches.

Business will continue to develop and improve filtering and other technologies that reduce spam. As spammers can change their tactics as quickly as industry develops new defensive techniques, technological responses to spam must continuously and rapidly adapt. Business is constantly improving the ability of these technologies to distinguish between spam and other communications, and developing products that are easier to use.

Business recognizes the significant challenge to information security presented by spam and has responded with innovations such as enterprise level network monitoring, traffic analysis and virus checking in order to protect information systems and networks. A new approach to spam is the use of "smart" systems that not only can adjust automatically to spammers' changing tactics, but can be customized to suit the preferences of individual users.

Governments should avoid mandating specific anti-spam technologies, and focus on creating and sustaining a climate in which business continues to innovate, develop and improve technological solutions to the ever-changing problem of spam.

- Governments should ensure that anti-spam measures are technology-neutral and, where relevant, based on standards agreed to by business. Governments should not mandate specific technological anti-spam measures, or try to force companies to adopt measures that cannot be supported in the marketplace.

- Governments should continue to allow Internet service providers (ISPs) and other companies to block spam on their respective networks and systems, keeping in mind the benefits of legitimate commercial e-mail.

[5] http://www.iccwbo.org/home/menu_electronic_business.asp

3. Industry's role: Business can best manage legitimate unsolicited commercial e-mail with industry codes of conduct and other self- regulatory tools

Businesses want to ensure the trust of their customers by sending them targeted and potentially interesting messages intended to begin or enhance a customer relationship. It is also in business' interest to maintain the usefulness of the Internet and associated communication technologies as a medium for responsible and acceptable commercial messages. Business can help free government resources to address spam by developing oversight and compliance mechanisms to manage legitimate unsolicited commercial e-mail using industry codes of conduct and other tools.

Industry codes, guidelines, and private sector best practice initiatives, such as the ICC Guidelines on Marketing and Advertising Using Electronic Media [6], the FEDMA European Code of Practice for the Use of Personal Data in Directing Marketing,[7] Antispam – A Guideline from The Confederation of Danish Industries and ITEK[8], the GBDe voluntary practices in its Recommendation on Unsolicited Electronic Communications[9], and Truste.org[10] are an effective way to spread best practices.

- Governments should respect and encourage industry codes of conduct and best practices that establish guidelines for the responsible business use of unsolicited commercial e-mails.

- Business should continue to use codes and best practices to educate more companies about acceptable direct marketing practices.

4. Government enforcement: Governments should ensure that relevant existing legislation covers all electronic messages and is effectively enforced

Business urges governments to adopt balanced legislative approaches as part of a toolkit of possible ways to combat spam. Governments should review existing laws and regulations to see if they sufficiently address spam.

New legislation or amendments, where needed, should focus on preventing illegitimate, fraudulent, or harmful messages. Measures should be drafted with care to reduce the volume of while preserving legitimate business use of the Internet as a communications and marketing medium. Laws should distinguish between harmful, fraudulent, misleading or illegitimate electronic communications sent by unknown parties from communications sent by responsible companies to individuals to create or sustain a customer relationship.

- Relevant legislation (for example, laws and regulations on fraud, consumer protection, unfair competition) should include definitions that prohibit activities such as the use of false or

[6] http://www.iccwbo.org/home/statements_rules/rules/1998/internet_guidelines.asp.
The ICC Guidelines are currently under revision to be finalized in June 2004.
[7] http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77-annex_en.pdf
[8] http://billed.di.dk/wimpfiles/lores/image.asp?objno=/298860.pdf
[9] http://www.gbde.org/spam03.pdf
[10] http://www.truste.org

misleading header information, false or misleading subject lines, fraudulent or claims or offers, the misuse of third-party domain names and IP addresses, and harvesting e-mail addresses through dictionary attacks or anonymous/automated collection procedures.

- The laws and policies on spam of the country from which a company is sending bulk commercial email should apply. Alternatively, but less preferably, the application and enforcement of laws or policies on spam should exclude bulk commercial email that is not primarily intended for recipients in that country. They should also not be enforced against a communication on the basis of a portion (e.g. a packet or series of packets) of that communication being *routed through* but not *destined for* a recipient in that country.

Effective enforcement by governments is essential. Private enforcement measures and private rights of action through the judicial system are also an important part of the fight against spam and should be upheld in law. Some countries have introduced rapid injunction procedures for both private and public enforcement actions.

- Governments should respect customer privacy and choice while allowing legitimate companies, including SMEs, to market their products and services.

- Governments should ensure they are able in law to impose effective fines or other penalties on spammers.

- Governments should focus on fraud and allocate sufficient resources to effectively enforce existing fraud laws with regard to electronic communications.

- Governments should have effective procedures for dealing with cross-border complaints.

- Governments should take every precaution to avoid subjecting companies to diverging, competing and possibly conflicting, legal obligations;

A template for effective and appropriate Law enforcement cooperation:

Effective and appropriate law enforcement cooperation should be pursued actively by governments instead of unnecessary cross-border application of laws. The Council of Europe Convention on Cybercrime and the OECD Guidelines provide models for pursuing such cooperation. A template for effective and appropriate law enforcement cooperation should ensure that:

1. A request for cooperation from one law enforcement agency to a law enforcement agency in another country should only be honoured if the alleged conduct is a violation of the laws of both the requesting and requested countries, i.e. dual criminality; and

2. A company should only be required to respond to and comply with requests from a law enforcement agency of the country where it is established and where the evidence is located. [11]

Business Actions

These action points were developed by ICC in conjunction with BIAC (Business and Industry Advisory Committee to the OECD) to complement the actions already proposed for governments.

- Business will work cooperatively with governments to increase awareness and use of workable opt-out solutions and mechanisms to report and deal with e-mail, instant messaging or SMS abuse.

- Business will continue to raise user awareness of how to reduce and deal with spam at the individual and enterprise level, particularly through initiatives such as the ICC Global Online Resource on Spam.

- Business will continue to develop technological solutions to spam.

- Business will use private enforcement actions against spammers where those actions are appropriate and likely to be effective.

- Business will continue to advocate effective and workable approaches to spam. To this end, we draw attention to the statements and marketing codes of the following business organizations International Chamber of Commerce (ICC), Federation of European Direct Marketing Association (FEDMA), Global Business Dialogue on Electronic Commerce (GBDe), and the Direct Marketing Association (DMA) and Antispam – A Guideline from The Confederation of Danish Industries and ITEK (spell it out).

- Business will continue to co-operate amongst industry associations to share and advocate policy and best practices globally.

- Business will continue to support and participate in international multi-stakeholder dialogue to develop practical approaches to combat spam.

Business looks forward to continued dialogue and coordinated action with governments to fight spam. This will reinforce the privacy and security of all users and ensure that the Internet remains a viable and attractive place to do business.

Document N° 373-22/114
2 December 2004 MvdL/MF/dfc

[11] For example, provisions on mutual assistance in the Council of Europe Convention on Cybercrime do not require companies to respond to a request made directly by an enforcement agency from a foreign country. Rather, the foreign law enforcement agency should seek the assistance of the law enforcement agency in the country of the company. The national agency could then seek the cooperation of the company in accordance with applicable process and procedural controls.

Section 3
Policy Statement focused on European Union Context
Employee privacy, data protection and human resources
(4 December 2003)

Section 4

Final Approved Version of Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries (controller to controller transfers)

Section 5
Issues Paper on Internationalized Domain Names
(7 July 2006)

Section 6
Policy Statement The impact of Internet Content regulation
(18 November 2002)

Section 7
Policy Statement: ICC Framework for consultation and drafting of Information Compliance obligations
(15 June 2006)

Section 8
Policy Statement: Open Source Software *(27 October 2005)*

Section 9
Deploying the next generation Internet: ICC Statement on the introduction of IPv6 *(2 December 2004)*

Section 10

Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data outside the EU

(5 July 2006)