



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: mvdld@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 them¹

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](http://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	<p>National aid programs</p> <p>Local infrastructure initiatives (e.g. city-wide wi-fi networks)</p> <p>“Digital Literacy” education and training initiatives</p>	<p>2005 WSIS “Tunis Agenda for the Information Society” Statement</p> <p>UN ICT Task Force GeSci initiative</p> <p>The European Union “i2010” initiative</p> <p>ITU-D conference for development of digital infrastructure (Doha action plan), March 2006</p> <p>ITU “Connect the World” global multistakeholder initiative</p> <p>G8 DOT Force Initiative Recommendations</p>	<p>Corporate “hybrid initiatives” combining philanthropy and direct investment</p> <p>Business support for telecommunications accessibility approach</p> <p>Private corporate investment initiatives (e.g. HP e-inclusion project, Cisco Networking Academy Programme)</p> <p>Computer Technology Industry Association (CompTIA) initiatives for IT skills development</p>

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
<p>Consumer protection</p>	<p>Education and awareness raising programmes</p> <p>National policy regime options:</p> <ol style="list-style-type: none"> 1. Regulation and legislation 2. Self-regulatory initiatives <p>National, regional and local law enforcement cooperation</p>	<p>2000 OECD Guidelines for Consumer Protection in the Context of E-commerce</p> <p>2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders</p> <p>APEC Voluntary Consumer Protection Guidelines for the Online Environment</p> <p>Bilateral and multilateral government law enforcement and cooperation internationally</p>	<p>Education and awareness raising programmes</p> <p>Self-regulatory codes and enforcement organizations (e.g. BBBOnline)</p> <p>Provision of alternative dispute resolution services</p> <p>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)</p>
<p>Content</p>	<p>National legislation on access to or the dissemination of certain content</p>	<p>OECD Workshop on Online Content</p> <p>European Union "Safer Internet Programme"</p>	<p>Self-regulatory schemes (e.g. Internet Content Rating Association, filtering technologies)</p> <p>Innovation and development of content filtering tools for use by parents, service providers, etc.</p>
<p>Contractual issues</p>	<p>Legislative measures to ensure legal validity and recognition of electronic contracts</p>	<p>UNCITRAL Model Law on Electronic Commerce</p> <p>UNCITRAL Draft convention on electronic contracting</p>	<p>Provision of alternative dispute resolution services.</p> <p>ICC E-Terms 2004 electronic contracting tools</p> <p>ICC Guide to e-contracting</p>



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



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



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



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



Issue	National government actions and initiatives	Intergovernmental organization actions and initiatives	Private sector and business actions and initiatives
<p>Privacy and cross-border flows of personal data</p>	<p>National privacy regime options:</p> <ol style="list-style-type: none"> 1. General and/or sectoral regulation 2. Omnibus and sectoral legislation 3. Self-regulatory initiatives <p>Education and awareness raising activities</p>	<p>OECD Guidelines for the protection of privacy and transborder flows of personal data</p> <p>OECD Privacy Online: policy and practical guidance</p> <p>OECD Privacy policy statement generator</p> <p>OECD work on Spam</p> <p>UN Guidelines for the regulation of computerized personal data files</p> <p>Council of Europe Convention</p> <p>European Commission Directive 95/46/EC</p> <p>APEC Privacy Framework</p>	<p>Education and awareness raising (e.g. ICC Global Spam Fighting Resource, ICC Privacy Toolkit)</p> <p>Self-regulatory codes and enforcement organizations (e.g. ICC Guidelines on Marketing and Advertising on the Internet, Truste, BBBOnline)</p> <p>ICC policy paper on Spam</p> <p>Provision of reporting and 'optout' services. (e.g. national direct marketing associations)</p> <p>Company codes of conduct / binding corporate rules</p> <p>Model contract clauses for cross-border transfers of personal data including the industry alternative model contract clauses for data transfers from the EU</p> <p>GBDe recommendations for protection of personal data</p> <p>Innovation of new technologies to protect information, mitigate SPAM, etc.</p>
<p>Taxation of e-commerce</p>	<p>National policies regarding the taxation of electronic commerce</p>	<p>OECD Technical Advisory Group's recommendations on current taxation treaties</p>	<p>Work of the OECD Technical Advisory Groups on Tax in partnership with business</p>



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



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.centri.org
Electronic Frontier Foundation	EFF	www.eff.org
European Commission IPv6 Task Force		www.ec.ipv6tf.org/in/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.sdn.un.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

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

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 relevant² guidelines will take measures including the following:

- When collecting personal data, follow the provisions in the ICC International Code on Direct Marketing³ 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 defraud 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 Media⁶, 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 ITEK⁸, the GBDe voluntary practices in its Recommendation on Unsolicited Electronic Communications⁹, and Truste.org¹⁰ 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)



International Chamber of Commerce

The world business organization

Policy Statement policy statement focused on European Union context

Employee privacy, data protection and human resources

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

I. Introduction

Businesses have always had to collect and use personal information from and about employees to comply with labour, tax and other laws, to administer benefits, to operate their businesses, and to serve their customers. This policy statement sets out the position of the International Chamber of Commerce (ICC) on the key issues relating to data protection and human resources, and provides recommendations for governments making policy in this area. While technological changes and new privacy laws have caused some re-examination of workplace privacy, the amount and scope of information about their employees that employers must process has changed very little over the years. ICC therefore urges governments to work closely with business to ensure that legislation and policy dealing with data protection in the human resources context strikes a workable balance between the legitimate interests of employers, customers, and society as a whole, and the privacy of employees.

Multinationals have to abide by the law and meet the expectations of their workers and of the marketplace in all countries in which they operate. They recognize that they must meet their data protection obligations toward employees and that those obligations do not disappear simply because the employees are networked together and their data is processed at a distant location. However, data protection obligations and individual employee rights should be balanced with the benefits of networking and enterprise-level information systems and other legal obligations and duties of employers to their customers, their shareholders, and society at large.

Regimes already established to protect personal data include, in their scope, employment-related data. Separate treatment for human resources data does not provide additional protection for individuals and can even reduce benefits to employees. The lack of clarity for both employers and employees of the many national policies and laws on workplace privacy is creating an unacceptable level of risk for business, particularly multinational business. It greatly increases companies' compliance burden without appreciably improving employees' privacy. ICC urges national governments and international organizations to recognize, as an alternative to formal legislation, solutions such as company codes of conduct/policies that protect employee data while allowing companies to utilize enterprise-level information systems designed to make business more efficient and benefit companies, employees and customers.

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

Governments, regulatory agencies and data protection authorities should coordinate closely with their international counterparts to prevent the emergence of a patchwork of different obligations. Governments should rely on industry to protect its human resource data effectively as protecting employees' personal data from misuse is vital to ensuring employee satisfaction. Governments should re-examine existing laws which have a bearing on employee privacy with a view to streamlining compliance burdens on employers and offering more flexible means for compliance. However, any government actions should first engage industry to determine the potential impact of any obligations.

ICC draws attention to the valuable work of the International Labour Organisation, which published its Code of Practice for the Protection of Workers' Personal Data in 1997.¹ This Code may be used as the starting point for further discussions between legislators, industry and employees.

II. Technological developments and new ways of working

Recent technological and business developments, such as the growth of the Internet (as well as private data networks and virtual private networks) and the deployment of enterprise resource management (ERM) information systems, allow for the development of new global business models offering the potential for organizations to offer more, and more efficient, products and services to their customers and employees. ERM information systems are designed to standardize the ways of working and decision-making throughout an enterprise. They permit the automated flow of information to all affected functions in the enterprise. Enterprise-wide communications and information systems typically entail central servers and host computers, as well as remote access by authorized persons located anywhere. The centralized nature of these systems permits the deployment of centralized and uniform controls that can facilitate compliance with corporate policies and review processes. Networking and enterprise-level information systems offer many benefits both to employees and businesses including increased efficiency and productivity, lower costs, and greater flexibility.

Enterprise-level information and communication systems can:

- Reduce the need for duplicating computer facilities in each office or plant location.
- Reduce the number of times a particular piece of data must be entered into a database and ensure greater accuracy and transparency.
- Reduce the number of software programs and database types that the company must support and that employees must learn, reducing costs and promoting efficiency.
- Increase the speed and efficiency of the processing of expenses and other employee claims and benefits.
- Speed up the delivery of data to managers and employees and give them direct access to the data they need.
- Allow centralized as well as local recruiting, and speed up the processing of applications,

¹ <http://www.ilo.org/public/english/protection/safework/cops/english/download/e000011.pdf>

requests, and orders.

- Permit more uniform and better enforced information policies, procedures, training, controls, and security across a corporate group, facilitating compliance with, for example, data protection codes and information security policies.
- Allow knowledge, experience and opportunities to be shared widely and almost immediately within a corporate group on a global scale.

Working practices have also changed dramatically in the last twenty years. Many employees now carry out some of their duties outside the workplace, for example, at remote sites such as clients' premises, while travelling, or at home. These employees need to be able to access the appropriate information while working remotely. Also, the complex clustering of functional working groups within enterprises is not necessarily consistent with the formal legal structure of the enterprise or even the formal employment arrangements, making it necessary to route employee data to other parts of the enterprise. Further, the boundaries between employees' work and private lives are being re-drawn as employees are able to work from home or be available for work-related communications outside office hours. Finally, outsourcing of functions such as payroll, recruitment and selection means that employees' personal data may need to be transferred to third parties in the course of normal business activities.

Employees clearly benefit in this evolving environment, enjoying, for example:

- Enhanced job security and prospects by improving the overall profitability of the company.
- Access to ideas and information from throughout the company, and more opportunities for distance learning and corporate training programs.
- Closer integration of employees at a distance from headquarters or from the larger plants and offices into the resources, culture, and personnel of the organization overall, and greater awareness of opportunities within the organization.
- Opportunities to readily view human resources information about themselves and update their personal data and their benefits choices.
- Flexible working hours or telecommuting opportunities, which allow employees to respond to child or family care situations.
- Greater choice and flexibility regarding benefits options, for example, with benefits plans that can be configured by the employee and automatically communicated to third-party benefits providers, rather than relying on the intervention of HR personnel.

The ability of business to make data transfers, particularly to third countries, is an essential part of global trade. As a result of varying national restrictions on transborder data flows, some companies have delayed implementing global enterprise information systems in, or including data from, countries that limit data flows of human resources data. Companies may also be required to restrict the access of employees in some countries to the full benefits of corporate Intranets. The outstanding issues surrounding crossborder transfers of personal data, including, but not limited to, employee data, need to be resolved as soon as possible so that companies, employees and economies as a whole can maximize the potential that technology developments and new ways of working offer.

III. Specific issues in data protection and human resources

Developing codes of conduct

Governments should allow companies to develop unified and comprehensive systems for human resource data management without imposing excessive obligations. Government or regulatory agency policies, or guidance from data protection authorities, should ensure that these integrated means for handling employee data worldwide can exist without impairing business efficiency. Governments should provide clear and practical guidance for the application of corporate codes, without the need for cumbersome registration or notification procedures, and with a streamlined approval process. Country-by-country approval processes, such as those currently used in the European Union, are a barrier to business and need to be addressed urgently.

Workplace monitoring

There are several reasons for the monitoring of employees which may vary from one employer, and situation, to another, such as:

- To detect, investigate, and prevent crime, such as theft, fraud or illegal use of software or the intellectual property of the employer or a third party.
- To prevent the unauthorized or unlawful disclosure of confidential business information, for example, trade secrets.
- To comply with obligations to prevent discrimination or sexual harassment under applicable laws, and prevent or reduce company exposure to liability for the unlawful acts of employees, particularly in relation to racist or sexist communications in the workplace.
- To maintain productivity and ensure the quality of products and services, and avoid damage to the company's reputation and goodwill.
- To comply with laws and regulations, e.g., workplace safety, labour, tax and other requirements.
- To ensure the integrity of information systems and compliance with company security and data protection policies.

Workplace monitoring is becoming acceptable and commonplace in many countries, although care needs to be exercised that the practice is consistent with local cultural values and traditions. Proportionate monitoring of electronic communications can be an essential part of corporate measures to foster the “culture of security” called for by the OECD Guidelines for the Security of Information Systems and Networks².

ICC supports lawful and fair monitoring of employee activities and communications. Employers should provide employees with notice of their policies governing the use of electronic communications, including policies on inspection and monitoring of communications, and employees should be made aware of any policy changes. It may be appropriate to provide notice

² <http://www.oecd.org/dataoecd/59/0/1946946.pdf>



to employees, or other individuals using the company's communication infrastructure, about the general circumstances under which monitoring might take place. However, prior information to an employee about specific investigations of suspected criminal activity or alleged contravention of company policies, is clearly counterproductive and should never be required.

There is considerable uncertainty as to employers' obligations and employee rights regarding workplace monitoring within some jurisdictions, and enormous variation between jurisdictions. Ill-defined restrictions on monitoring leave employers uncertain about what is permissible. This lack of clarity creates an unacceptable level of risk and potential liability for employers, and does not assist employees in knowing what level and type of privacy in the workplace they may legitimately expect. Moreover, it fails to advance worldwide interests in safeguarding important network, information and physical infrastructures, or in protecting consumers (including vulnerable consumers like children or the elderly). In many cases it is not possible to clearly delineate an employee's professional and personal use of business equipment to distinguish what types of activities may be monitored without imposing unreasonable burdens on employers. ICC urges national governments and international organizations to work with business to clarify these issues and recognize solutions such as company codes of conduct/policies as an alternative to formal legislation. These principles should be applied to other types of monitoring and surveillance used by companies for valid business purposes, such as video surveillance, building access control systems or performance monitoring systems.

Recruitment and selection

Business should not be prevented from making appropriate, focused and reasonable use of pre-employment screening procedures for prospective employees, provided the prospective employees are made aware that this may happen. These searches can include fact-checking of personal details provided by an applicant and an investigation of the broad suitability of the applicant for the post being considered. Increasingly, companies are legally required to vet employees in the areas of health, childcare, teaching, finance, or privately provided security and law enforcement service provision.

Restrictions on pre-employment screening may undermine necessary security measures and prevent businesses protecting themselves from the potential of fraud, damage to reputation, or other harms to businesses, their employees or customers. These restrictions may also leave companies vulnerable to liability claims from third parties if incompletely vetted employees cause harm.

In some jurisdictions employers face potential liability if they fail to conduct thorough checks on employees who are able to access the sensitive information of customers, for example, financial information, or who deal with vulnerable citizens such as health care subjects. It is in the interest of society as a whole to make sure that employers are legally able to conduct a thorough and proper review of employees and prospective employees, in the exercise of due diligence, and, using network resources, to transfer the information to appropriate human resources personnel in the context of hiring and other decisions.

Use of business contact data

Business has a legitimate need to freely use business information that may contain limited personal information, for example, an individual's name, job title, and work contact details. This

use of limited personal information for business purposes does not compromise the legitimate expectations of individuals with respect to harmful use of personal data, and is an essential part of acceptable business practice. Governments should not include business information of this kind in the scope of privacy regimes created to protect other personal data.

Facilitating cross-border data transfers

Companies in all countries and sectors need to transfer personal data from countries that regulate the export of personal data. Companies are able to both maximize the benefits attained by centrally locating human resource data and protect this data by establishing an appropriate access plan based on their global management structure. Business, in general, closely controls the individuals that have access to sensitive internal human resource data. The level and type of access to data, rather than its physical location, should be the primary focus in determining the risks of misuse of personal data. ICC urges governments to take a non-discriminatory view of different approaches to privacy protection, for example, legislative or self-regulatory approaches, and to encourage free flows of information where personally identifiable data is protected effectively. Governments that nevertheless choose to restrict employee data flows should support the broadest set of mechanisms possible to facilitate legitimate data transfers, for example, the use by companies of informed consent, contracts, and codes of conduct/company policies.

Consent

Fair processing of employee data can often be based on the needs of the employment contract, compliance with the legal obligations of the employer, and/or the legitimate interests of the employer or a third party which override the privacy interests of the employee. However, in circumstances not covered by these grounds, for example, transborder data flows, the employer must be allowed to rely on the principle of informed, unambiguous consent. Companies routinely include disclosure and consent provisions in their documentation for new employees for a range of different reasons including benefits programmes, and network access and monitoring. Consumers routinely consent to contractual provisions that they have no opportunity to negotiate, and consent in this context is not considered invalid unless the terms are unduly burdensome or onerous. The same should hold true for employees.

Where employee consent is required or used, the legal requirements for lawful consent should not exceed the principle of informed, unambiguous consent, and should be in full agreement with national requirements regarding the expression of will in the employment context. Explicit consent, especially written consent, should be reserved for extraordinary circumstances only, where the interests of the employee are seriously at risk, such as the processing of sensitive data such as health data. Nonetheless, employees should not be permitted to prevent a company from efficiently administering health and other benefits as long as adequate safeguards to protect privacy are in place.

Sensitive data

Where it is necessary for essential business purposes, or to comply with an employer's obligations under the law, companies should be permitted to request and retain employees' sensitive data. The employer must clearly inform the employee of the purpose for which the data are processed and should obtain the employee's consent if required under local law. However, employees should not be allowed to prevent the collection of vital information that



may prove essential to employers in meeting their legal obligations to their customers, to the public, and to fellow employees.

IV. Conclusion

Effectively protecting employees' personal data from misuse is vital to ensuring employee satisfaction. At the same time, the Internet and new resource management technologies have created many advantages to business and their employees in terms of cost savings, increased efficiency and productivity, enhanced benefit packages, security and convenience. Flexibility and the ability to accommodate differences in interpreting privacy in the workplace are needed to facilitate access to information, communications, and commerce on a global scale.

Document N° 373-22/112

4 December 2003 MF/dfc

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)**



International Chamber of Commerce

The world business organization

Department of Policy and Business Practices

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

Commission on E-Business, IT & Telecoms

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



Table of Contents

I.	Introduction	3
II.	Frequently Asked Questions	4
III.	Standard Contract Clauses	7
	ANNEX A: Data Processing Principles.....	13
	ANNEX B: Description of the Transfer	15
	Illustrative Commercial Clauses (Optional)	16



I. Introduction

On December 27, 2004, the European Commission recognized a set of standard contractual clauses proposed by seven leading business associations (including ICC)¹ as providing an “adequate level of data protection” under the EU Data Protection Directive 95/46/EC for transferring personal data outside the EU.

The Commission’s approval means that the clauses are officially recognized as granting full protection under EU data protection law for personal data that is transferred from all Member States of the European Union. The alternative clauses give business an important additional tool to satisfy the EU’s stringent restrictions on data exports, and provide additional protections to personal data beyond those contained in the Commission’s present standard contractual clauses. These FAQs answer some preliminary questions regarding the clauses.² The clauses themselves are available below and on the Commission’s web site.³

¹ The associations are the American Chamber of Commerce to the European Union in Brussels (AmCham EU); Confederation of British Industry (CBI); European Information, Communications and Consumer Electronics Technology Industry Association (EICTA); Federation of European Direct and Interactive Marketing (FEDMA); International Chamber of Commerce (ICC); International Communication Round Table (ICRT); and the Japan Business Council in Europe (JBCE).

² These FAQs have been drafted by Christopher Kuner, Chairman, ICC Task Force on Privacy and the Protection of Personal Data.

³ See http://www.europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm.



II. Frequently Asked Questions

What is the purpose of the clauses?

European data protection law prohibits the transfer of personal data (for example, employee records, customer data, and company information collected in the scope of a “due diligence” procedure) outside the EU to countries that do not enjoy an “adequate level of data protection”. One of the ways to provide for such an adequate level of protection for transfers to countries that have not been formally found to be “adequate” by the EU is for the data exporter in the EU and the data importer outside the EU to conclude a data transfer agreement containing protections for the data. In 2001, the European Commission published a set of standard contractual clauses for controller-to-controller transfers (available on the Commission web site given above). The Commission’s adequacy decision means that the new clauses provide adequate protection for data transfers just as the existing clauses do.

Does my company have to use the clauses?

No, use of the clauses, like use of the Commission’s existing clauses, is purely voluntary.

What about the Commission’s existing clauses?

The Commission’s clauses from 2001 remain in effect, so that companies now have two sets of clauses to choose from.

When can my company start using the Clauses?

The clauses are legally valid for transfers as from April 1, 2005.

What types of transfers are covered by the clauses?

The clauses may be used for all transfers from a data controller in the EU to another data controller outside the EU (a data controller is an entity that determines the purposes and means of data processing). For example, a data importer that processes personal data from the EU solely at the direction of the European data exporter and without any discretion as to the purposes and means of processing is generally not considered a data controller.

Which countries are covered by the clauses?

The clauses cover data transfers from all EU member states. The clauses may be used for transfers to all countries outside the EU that have not been formally found by the European Commission to offer an “adequate level of data protection”. Thus, they may be used for transfers from the EU to all countries EXCEPT the following ones, for which the use of contractual clauses is not necessary since such countries already offer an adequate level of data protection:

- The twenty-five EU Member States (currently Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom);
- The countries of the European Economic Area (Iceland, Liechtenstein, and Norway);



- The following countries that have been found by the EU to offer an adequate level of protection: Argentina, Canada, Guernsey, the Isle of Man, Switzerland, and the United States (but only for transfers to companies that are members of the US “safe harbour” arrangement).

What are the major differences between the Commission’s existing clauses and the new alternative clauses?

The new clauses grant “adequate protection” under EU law just as the Commission’s existing clauses do, but arrive at the same level of protection using a different route. The following are some of the main differences between the Commission’s existing clauses and the new alternative standard clauses:

1. The Commission Decision approving the new clauses limits the ability of the data protection authorities to block data flows in cases where data importers are unable to perform the contract because doing so would put them in violation of their home country law in areas such as tax reporting and money laundering.
2. *Liability*: The alternative clauses do not contain a joint and several liability clause, but instead place due diligence requirements on both importer and exporter (e.g., Clauses I.b. and II.f), and make each party liable only for the damages it caused (Clause III.a).
3. *Access rights*: The alternative clauses allow access to be denied for requests “which are obviously abusive based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter” (Annex A.5).
4. *Third Party Beneficiary Rights*: The alternative clauses (Clause III.b) do not specifically require the parties to waive objections to consumer organizations bringing suit on behalf of data subjects as do the Commission’s existing clauses (Clause 3). Also, the alternative clauses allow direct suits by data subjects against the importer only if the exporter has not taken action to enforce the clauses within a reasonable period (normally one month).
5. *Making clauses available to data subjects*: The alternative clauses limit to the exporter the obligation to provide a copy of the clauses (Clause I.e), and then allow the exporter to remove confidential information from the clauses.
6. *Handling of complaints*: The alternative clauses allow, in effect, for the exporter and the importer to “outsource” to the importer the task of responding to inquiries from national data protection authorities (DPAs) (Clauses I.d and II.e).
7. *Monitoring compliance with local law*: Alternative clause II.c limits the importer’s obligation to warrant that local law does not prevent it from fulfilling its obligations under the contract to knowledge the importer has at the time it enters into the clauses, and to legal obligations “which would have a substantial adverse effect” on its compliance with the clauses. The alternative clauses also oblige the importer to notify only the exporter if it becomes aware of a conflicting legal obligation.
8. *Audits*: The alternative provision on auditing (Clause II.g) gives the data importer more rights than the Commission’s does. For instance, in the alternative clauses the exporter’s request for an audit is limited by several reasonableness requirements, and the auditor need not be agreed to by the DPA of the exporter’s country as in the Commission’s clause.



9. *Cooperation with DPAs:* The Commission's clauses require the importer to abide by "the advice" of the DPA, which term is dangerously vague. The alternative clauses require compliance with "a decision" of a competent court or a DPA "which is final and against which no further appeal is possible" (Clause V.c).
10. *Termination:* The alternative clauses contain detailed rules for termination and concerning the rights and obligations of the parties in the event of termination (Clause VI); the Commission's clauses contain only a single sentence dealing with termination.
11. *Variation of the clauses:* The alternative clauses allow the updating of factual information in Annex B, and for additional commercial provisions to be added. In addition, the alternative clauses allow for more flexible administration of the clauses, by explicitly allowing for the execution of additional annexes to cover additional transfers or for a single annex to cover multiple transfers.
12. *Notice of onward transfers:* The alternative Clause II.i.iii allows the importer to tell the data subject that the countries to which data will be further transferred "may have different data protection standards", rather than saying that "there is not an adequate level of protection of the privacy of individuals" in such countries as the Commission's clauses require.



III. Standard Contract Clauses

Standard Contractual Clauses for the Transfer of Personal Data from the Community to Third Countries (controller to controller transfers)

Data Transfer Agreement

Between

_____ (name)
_____ (address and country of establishment)
Hereinafter “Data Exporter”

and

_____ (name)
_____ (address and country of establishment)
Hereinafter “Data Importer”

each a “Party”, together “the Parties”

Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data/sensitive data', 'process/processing', 'controller', 'processor', 'Data Subject', and 'Supervisory Authority/Authority' shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby 'the Authority' shall mean the competent data protection authority in the territory in which the data exporter is established);
- (b) 'the Data Exporter' shall mean the controller who transfers the Personal Data;
- (c) 'the Data Importer' shall mean the Controller who agrees to receive from the Data Exporter personal data for further processing in accordance with the terms of these Clauses and who is not subject to a third country's system ensuring adequate protection;
- (d) 'Clauses' shall mean these Contractual Clauses, which are a free-standing document that does not incorporate commercial business terms established by the Parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the Clauses.

I. Obligations of the Data Exporter

The Data Exporter warrants and undertakes that:

- a) The Personal Data have been collected, processed, and transferred in accordance with the laws applicable to the Data Exporter.



- b) It has used reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these Clauses.
- c) It will provide the Data Importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the Data Exporter is established.
- d) It will respond to enquiries from Data Subjects and the Authority concerning processing of the Personal Data by the Data Importer, unless the Parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Responses will be made within a reasonable time.
- e) It will make available, upon request, a copy of the Clauses to Data Subjects who are third party beneficiaries under Clause III., unless the Clauses contain confidential information, in which case it may remove such information. Where information is removed, the Data Exporter shall inform Data Subjects in writing of the reason for removal and of their right to draw the removal to the attention of the Authority. However, the Data Exporter shall abide by a decision of the Authority regarding access to the full text of the Clauses by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Data Exporter shall also provide a copy of the Clauses to the Authority where required.

II. Obligations of the Data Importer

The Data Importer warrants and undertakes that:

- a) It will have in place appropriate technical and organisational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- b) It will have in place procedures so that any third party it authorises to have access to the Personal Data, including processors, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Data Importer, including a data processor, shall be obligated to process the Personal Data only on instructions from the Data Importer. This provision does not apply to persons authorised or required by law or regulation to have access to the Personal Data.
- c) It has no reason to believe, at the time of entering into these Clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these Clauses, and it will inform the Data Exporter (which will pass such notification on to the Authority where required) if it becomes aware of any such laws.
- d) It will process the Personal Data for purposes described in Annex B, and has the legal Authority to give the warranties and fulfil the undertakings set out in these Clauses.
- e) It will identify to the Data Exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the Personal Data, and will cooperate in good faith with the Data Exporter, the Data Subject and the Authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the Data Exporter,



or if the Parties have so agreed, the Data Importer will assume responsibility for compliance with the provisions of Clause I.(e).

f) At the request of the Data Exporter, it will provide Data Exporter with evidence of financial resources sufficient to fulfil its responsibilities under Clause III. (which may include insurance coverage).

g) Upon reasonable request of the Data Exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the Data Exporter (or any independent or impartial inspection agents or auditors, selected by the Data Exporter and not reasonably objected to by the Data Importer) to ascertain compliance with the warranties and undertakings in these Clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Data Importer, which consent or approval the Data Importer will attempt to obtain in a timely fashion.

h) It will process the Personal Data, at its option, in accordance with:

- (i) the data protection laws of the country in which the Data Exporter is established; or
- (ii) the Relevant Provisions⁴ of any Commission Decision pursuant to Article 25(6) of Directive 95/46/EC, where the Data Importer complies with the relevant provisions of such an authorization or Decision and is based in a country to which such an authorization or Decision pertains, but is not covered by such authorization or Decision for the purposes of the transfer(s) of the Personal Data;⁵ or
- (iii) the data processing principles set forth in **Annex A**.

Data Importer to indicate which option it selects: _____

Initials of Data Importer: _____

i) It will not disclose or transfer the Personal Data to a third party Data Controller located outside the European Economic Area (EEA) unless it notifies the Data Exporter about the transfer and

- (i) the third party Data Controller processes the Personal Data in accordance with a Commission decision finding that a third country provides adequate protection, or
- (ii) the third party Data Controller becomes a signatory to these Clauses or another data transfer agreement approved by a competent authority in the EU, or
- (iii) Data Subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which Data is exported may have different data protection standards, or

⁴ “Relevant Provisions” means those provisions of any authorization or Decision except for the enforcement provisions of any authorization or Decision (which shall be governed by these Clauses).

⁵ However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.



- (iv) with regard to onward transfers of sensitive data, Data Subjects have given their unambiguous consent to the onward transfer.

III. Liability and Third Party Rights

a) Each Party shall be liable to the other Party for damages it causes by any breach of these Clauses. Liability as between the Parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each Party shall be liable to Data Subjects for damages it causes by any breach of third party rights under these Clauses. This does not affect the liability of the Data Exporter under its data protection law.

b) The Parties agree that a Data Subject shall have the right to enforce as a third party beneficiary this Clause and Clauses I.(b), I.(d), I.(e), II.(a), II.(c), II.(d), II.(e), II.(h), II.(i), III.(a), V., VI.(d), and VII. against the Data Importer or the Data Exporter, for their respective breach of their contractual obligations, with regard to his Personal Data, and accept jurisdiction for this purpose in the Data Exporter's country of establishment. In cases involving allegations of breach by the Data Importer, the Data Subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer; if the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the Data Subject may then enforce his rights against the Data Importer directly. A Data Subject is entitled to proceed directly against a Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these clauses (the Data Exporter shall have the burden to prove that it took reasonable efforts).

IV. Law Applicable to the Clauses

These Clauses shall be governed by the law of the country in which the Data Exporter is established, with the exception of the laws and regulations relating to processing of the Personal Data by the Data Importer under Clause II.(h), which shall apply only if so selected by the Data Importer under that Clause.

V. Resolution of Disputes with Data Subjects or the Authority

a) In the event of a dispute or claim brought by a Data Subject or the Authority concerning the processing of the Personal Data against either or both of the Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The Parties agree to respond to any generally-available non-binding mediation procedure initiated by a Data Subject or by the Authority. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation, or other dispute resolution proceedings developed for data protection disputes.

c) Each Party shall abide by a decision of a competent court of the Data Exporter's country of establishment or of the Authority which is final and against which no further appeal is possible.



VI. Termination

a) In the event that the Data Importer is in breach of its obligations under these Clauses, then the Data Exporter may temporarily suspend the transfer of Personal Data to the Data Importer until the breach is repaired or the contract is terminated.

b) In the event that:

- (i) the transfer of Personal Data to the Data Importer has been temporarily suspended by the Data Exporter for longer than one month pursuant to paragraph a);
- (ii) compliance by the Data Importer with these Clauses would put it in breach of its legal or regulatory obligations in the country of import;
- (iii) the Data Importer is in substantial or persistent breach of any warranties or undertakings given by it under these Clauses;
- (iv) a final decision against which no further appeal is possible of a competent court of the Data Exporter's country of establishment or of the Authority rules that there has been a breach of the Clauses by the Data Importer or the Data Exporter; or
- (iv) a petition is presented for the administration or winding up of the Data Importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate these Clauses, in which case the Authority shall be informed where required. In cases covered by i), ii), or iv) above the Data Importer may also terminate these Clauses.

c) Either Party may terminate these Clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the Data Importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country. d) The Parties agree that the termination of these Clauses at any time, in any circumstances and for whatever reason (except for termination under Clause VI.(c)) does not exempt them from the obligations and/or conditions under the Clauses as regards the processing of the Personal Data transferred.

VII. Variation of these Clauses

The Parties may not modify these Clauses except to update any information in **Annex B**, in which case they will inform the Authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the Personal Data are specified in **Annex B**. The Parties agree that **Annex B** may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent



regulatory or government agency, or as required under Clause I.(e). The Parties may execute additional Annexes to cover additional transfers, which will be submitted to the Authority where required. **Annex B** may, in the alternative, be drafted to cover multiple transfers.

Dated: _____

for DATA IMPORTER

for DATA EXPORTER

.....
.....
.....

.....
.....
.....



ANNEX A: Data Processing Principles

1. **Purpose limitation** - Personal Data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the Data Subject.
2. **Data quality and proportionality** - Personal Data must be accurate and, where necessary, kept up to date. The Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. **Transparency** - Data Subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the Data Exporter.
4. **Security and confidentiality** - Technical and organisational security measures must be taken by the Data Controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the Data Controller, including a processor, must not process the data except on instructions from the Data Controller.
5. **Rights of access, rectification, deletion and objection** - As provided in Article 12 of Directive 95/46/EC, Data Subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter. Provided that the Authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organizations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the Data Subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data Subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these Principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment, or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A Data Subject must also be able to object to the Processing of the Personal Data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the Data Importer, and the Data Subject may always challenge a refusal before the Authority.



6. **Sensitive Data** - The Data Importer shall take such additional measures (e.g., relating to security) as are necessary to protect such Sensitive Data in accordance with its obligations under Clause II.

7. **Data used for Marketing Purposes** - Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the Data Subject at any time to 'opt-out' from having his data used for such purposes.

8. **Automated Decisions** - For purposes hereof 'Automated Decision' shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a Data Subject or significantly affects a Data Subject and which is based solely on automated processing of Personal Data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Data Importer shall not make any Automated Decisions concerning Data Subjects, except when:

a.

- i) such decisions are made by the Data Importer in entering into or performing a contract with the Data Subject, and
- ii) the Data Subject is given an opportunity to discuss the results of a relevant Automated Decision with a representative of the party making such decision or otherwise to make representations to that party.

or

b. Where otherwise provided by the law of the Data Exporter.



ANNEX B: Description of the Transfer

[To be completed by the Parties]

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

.....
.....
.....
.....

Purposes of the transfer[s]

The transfer is made for the following purposes:

.....
.....
.....
.....

Categories of data

The Personal Data transferred concern the following categories of data:

.....
.....
.....
.....

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

.....
.....
.....
.....

Sensitive Data (if appropriate)

The Personal Data transferred concern the following categories of Sensitive Data:

.....
.....
.....
.....

Data protection registration information of Data Exporter (where applicable)

.....
.....

Additional useful information (storage limits and other relevant information)

.....
.....

Contact points for data protection enquiries

Data Importer

.....
.....
.....

Data Exporter

.....
.....
.....



Illustrative Commercial Clauses (Optional)

Indemnification between the Data Exporter and Data Importer:

“The Parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these Clauses. Indemnification hereunder is contingent upon (a) the Party(ies) to be indemnified (the “Indemnified Party(ies)”) promptly notifying the other Party(ies) (the “Indemnifying Party(ies)”) of a claim, (b) the Indemnifying Party(ies) having sole control of the defence and settlement of any such claim, and (c) the Indemnified Party(ies) providing reasonable cooperation and assistance to the Indemnifying Party(ies) in defence of such claim.”

Dispute Resolution between the Data Exporter and Data Importer (the Parties may of course substitute any other alternative dispute resolution or jurisdictional clause):

“In the event of a dispute between the Data Importer and the Data Exporter concerning any alleged breach of any provision of these Clauses, such dispute shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be []. The number of arbitrators shall be [].”

Allocation of Costs:

“Each Party shall perform its obligations under these Clauses at its own cost.”

Extra Termination Clause

“In the event of termination of these Clauses, the Data Importer must return all Personal Data and all copies of the Personal Data subject to these Clauses to the Data Exporter forthwith or, at the Data Exporter's choice, will destroy all copies of the same and certify to the Data Exporter that it has done so, unless the Data Importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The Data Importer agrees that, if so requested by the Data Exporter, it will allow the Data Exporter, or an inspection agent selected by the Data Exporter and not reasonably objected to by the Data Importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours.”

Section 5

Issues Paper on Internationalized Domain Names

(7 July 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

Issues Paper on Internationalized Domain Names

The introduction of Internet domain names in LDH (Letters Digits Hyphen)¹ characters is the subject of much controversy and debate. Some contend that it is an almost trivial exercise while others argue that it is a tremendously complex task that if done too hastily or without proper planning threatens the integrity and stability of the Internet. The Internet Engineering Task Force (IETF) has produced a number of 'Requests for Comments (RFCs)' on the topic (see <http://www.rfc-editor.org/rfc/rfc3490.txt>) that provide guidance on the issue.

The Task Force on the Internet and IT Services has developed this Issues Paper on internationalized domain names (IDNs) to explain the need for IDNs in a manner that ensures the flexibility, stability, and global interoperability of the Internet. Given the current existence of numerous languages and some 241 top-level domain names (TLDs), there is no question that it is a huge and complicated task. Indeed, it is one that could quickly become mired in boundless problems.

This paper examines a number of the issues surrounding IDNs, such as the need for their introduction, the technical challenges, and the risks to the current domain name system. It also addresses their impact on business, including the ability of companies to protect their intellectual property. Finally, it outlines policy issues such as the impact on IDN's on current policies governing the domain name system.

What are Internationalized Domain Names?

A domain name is the unique character-based label assigned to a numbered address. Although domain names are used in a number of different applications, in the context of this paper the Domain Name System (DNS) resolves and identifies the address and points a browser to a particular computer containing the user's requested data.

¹ The universal set of characters a-z, 0-9, hyphen and dot.

When a user enters a domain name in his browser, e.g., iccwbo.org, the user's computer accesses the global DNS directory to find the corresponding Internet Protocol Address (IP Address) of the website. On finding the IP Address, the user's computer is then able to contact and communicate with the computer bearing the IP Address corresponding to the iccwbo.org domain name. In effect, the domain name is simply the IP Address, represented in an easy to remember form, of the computer where ICC's data is held for public, or even private, access. The DNS allows the user's computer to replace the text-based label iccwbo.org with the IP Address and thus, locate and communicate with the ICC computer over the global Internet.

A domain name consists of both low level and top-level domain (TLD) name components. In the domain name "iccwbo.org", the low level domain name is "iccwbo", whilst the top level domain is ".org". There are different types of top-level domain names; generic TLDs (gTLD) such as .org, .com, .info, and country code TLD (ccTLD) such as .uk (United Kingdom), .fr (France), .jp (Japan).

Since the original language and characters available for use in computers and the Internet were based on ASCII (American Standard Code for Information Exchange)² codes/characters which use Latin characters, domain names were restricted initially to the LDH subset of ASCII characters or through the transliteration of non-Latin based languages into this subset.

Subsequently, the introduction of UNICODE³, "provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language."⁴ has created a uniform foundation for global software irrespective of language. UNICODE now comprises 96,382 characters from currently recognized scripts of the world. The standard is continuously upgraded to add new characters and character sets. New, and what may be described as non-transliterated Internationalized Domain Names, take advantage of this technological facility and allow the use of domain names in character sets other than LDH characters

Domain names can be 'internationalized' by allowing non-LDH characters in the domain. Domain names that may have appeared as "Urdu.com" can now appear as:

"اردو .com"

"اردو .com.pk"

"اردو .pk"

and even

"اردو .پک"

Different TLDs operators are currently offering Internationalized Domain Names. The question now is not how to enable internationalization of domain names but how to ensure that the processes for development, maintenance, upgrade and resolution proceed in a manner that will preserve the stability, integrity and security of the Internet. Specifically, it is necessary to have a uniform encoding of IDNs regardless of the specific

² ASCII (American Standard Code for Information Interchange). The ASCII characters are Latin or Roman language characters with a maximum of 128 defined alpha, numeric and special characters.

³ For more information: www.unicode.org

⁴ www.unicode.org/standards/WhatIsUnicode.html. Accessed June 20, 2006.



application that is using them. Browsers, as used in this paper, are only one example of such an application.

It is important, however, that the reader does not come away with the impression that providing for IDNs in the Domain Name System will resolve all issues with regard to the use of non-LDH characters. Mail systems are an example of an application that will require extensive modification to accommodate the use of IDNs.

The Case for Internationalized Domain Names

The demand for IDNs is based on the desire for increased access to the information and knowledge available online. Much of the world's population today does not use, or even recognize, Latin characters.

A multilingual Internet will foster an inclusive, democratic, legitimate, respectful, and locally empowering Information Society. In this regard, it can be said that what is truly needed are localized domain names – or, the ability to access the Internet in one's native language. To offer localized domain names, the Domain Name System (DNS) must be multilingual. Of course, the ability to obtain useful content in an individual's native language is a significant issue, but beyond the scope of this paper.

Non-LDH domain names are also necessary to safeguard the cultural and linguistic integrity of names, brands and trademarks represented in native character scripts. Companies and individuals in societies that use non-Latin characters will be able to globally preserve their unique web-identities.

Example:

A Japanese person's name “ $\square\square$ ” is transcribed as “hirofumi” in Roman letters. On the Internet, where only LDH characters can be used, he is “hirofumi”, just like other people named “hirofumi” but whose names may use different Japanese characters such as “ $\square\square$ ” or “ $\square\square$ ”. In fact, there may be over 100 different Japanese representations that will end up being denoted simply as “hirofumi” in LDH space. Consequently, in the LDH world, the person in question is just one “hirofumi” of many other Japanese “hirofumis”, although in his native Japanese characters he would be clearly differentiated.”⁵

While internationalized domain names will certainly help in achieving many objectives of developing countries, they cannot be considered to be the sole bridge for the digital divide. It is also important to consider the challenges posed by the fact that many people do not have access to computers in general and the Internet in particular. It is those who have access to both but are unable to practically use computers or the Internet due to language restrictions that are the ones most affected by the lack of internationalization.

⁵ Paragraph 14 of the Multilingual Domain Names: Joint ITU / WIPO symposium in association with the Multilingual Internet Names Consortium - <http://www.itu.int/mlds/briefingpaper/>



General Issues and Concerns

Technical Issues

There are substantial technical issues surrounding the introduction of IDNs, many of which are quite complex. The technical community is working toward their resolution. Rather than trying to include them specifically in this paper, the reader is encouraged to consult the Internet Engineering Task Force (IETF) paper at <http://www.ietf.org/Internet-drafts/draft-iab-idn-nextsteps-02.txt>.

This document describes some of the issues in detail and outlines the areas where further work is needed.

Intellectual Property Issues

The possibility for confusion among domain names raises several intellectual property issues. Several languages contain strings of characters that have equivalent or near-equivalent meanings. Use of such character strings in IDNs might lead to domain names that are similar phonetically, visually or across various character tables.

While classification of goods and services allows the use of a trademarked brand that might be similar or identical to another as long as they relate to a separate class of goods and services, this is not the case with respect to IDNs where there is no classification of domain names. Avoiding conflict and having a uniform globally enforceable dispute resolution policy is imperative for an efficient continued working of the DNS.

Lack of interoperability and coordination between registration authorities can lead to concerns by owners of domain names who must retain the ability to protect their trademark, trade name or brand. The ability of registration authorities to transfer domain names in case of breach of good faith on the part of respondents is essential, as is effective enforcement. Failure to resolve these issues will make the implementation of IDNs prohibitively expensive for business in trying to protect their IP rights.

The Internet Corporation for Assigned Names and Numbers (ICANN) and the World Intellectual Property Organization (WIPO) have already had to deal with the various issues that arise out of trademark and intellectual property disputes in IDNs. ICANN has contributed to the resolution of disputes in this area through the adoption of the Rules for Uniform Domain Name Dispute Resolution Policy (UDRP) on 24 October 1999, which has been used by WIPO in deciding cases on IDNs. The UDRP applies equally to both registered as well as unregistered trademarks. WIPO has, to date, decided 45 cases of non-ASCII Domain Names using Chinese, Dutch, French, German, Japanese, Korean, Norwegian, Spanish and Swedish languages.

However, some feel the UDRP still needs reform in the area of IDNs. For instance, use of the UDRP is driven by the existence of bad faith and lack of legitimate right to a domain name. A problem arises when both parties are bona fide and have conflicting legitimate rights and wish to or are using the domain name in good faith. This can have a substantial impact on business when faced with competitors to domain names that may phonetically sound or visually depict confusingly similar trademarks. This issue needs to be considered in order to have a system that addresses the disparate Internet scenarios that exist.



Security Issues

The possibility of confusion between phonetically similar or visually similar IDNs may be used for spoofing⁶ or phishing⁷ as well as cyber-squatting⁸. While such practices are possible within the LDH DNS, recently cyber criminals have taken advantage of the increased vulnerability in IDNs and the IDN system to confuse users regarding which web address or web page they are visiting. It is important for business to be aware of such vulnerabilities when managing their companies. In addition, there will be a need for industry support for development of solutions to the problem through technical and policy initiatives.

Language issues

The foundation for internationalization of computers and the Internet depends upon the availability and usage of character sets and character tables that are mapped to a universally recognized system such as UNICODE.⁹ However, the diaspora effect on languages, character tables and sets may lead to differences in national, official, regional, local and diasporan languages, causing further confusion and conflict for intellectual property in trade names, trademarks and brands.

For example, some Chinese characters have two representations – a traditional Chinese character and a simplified Chinese character. Correspondence between a traditional Chinese character and a simplified Chinese character is not one-to-one, and while they are usually used in mainland China in place of traditional Chinese characters, simplified Chinese characters are seldom used in Taiwan or Hong Kong. Such issues clearly will be difficult to decide, dictate or solve by regional, local or linguistic groups, since there will inevitably be conflict within such groups.

There are a number of organizations and consortiums attempting to resolve these differences. The Multilingual Internet Names Consortium (MINC)¹⁰ is one such group that has been active in raising the issue and in coordinating and compiling a number of language groups. The Unicode Consortium is a transparent, open and global institution that maintains the global Standard¹¹ for Languages character sets and tables. The Consortium cooperates with the World Wide Web Consortium (W3C) and International Organization for Standardization (ISO)¹² and liaises with ISO to ensure synchronization of the Unicode Standard with the International Standard ISO/IEC 10646. The Unicode Consortium includes major computer corporations, software producers, database vendors, research institutions, international agencies, various user groups, educational institutions, governments and interested individuals. The Unicode Consortium enables a globally unified and effective solution to problems related to character sets that ensure

⁶ A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

⁷ A technique whereby the websites of known institutions are entirely or partly copied and e-mails are used to obtain private or confidential data of the customers of those institutions. The request to provide those data is often motivated by so-called safety measures or the need to update data banks.

⁸ Cyber-squatting is the act of registering a popular Internet address, usually a company name, with the intent of selling it to its rightful owner.

⁹ Character Sets is a widely used term and may mean any or a combination of the following three: character repertoire, character code, and character encoding. A tutorial on character code issues is available at <http://www.cs.tut.fi/~jkorpela/chars.html>

¹⁰ www.minc.org

¹¹ Unicode Standard 4.0

¹² www.iso.org



that the standard is implemented not just over regional or local jurisdictions but throughout software, computers and the Internet.

Introduction of Uniform Resource Identifiers (URI) may further assist in the internationalization of the Internet. A Uniform Resource Identifier (URI) is a compact string of characters for identifying an abstract or physical resource.¹³ URIs may contain information from all kinds of protocols or formats that use characters beyond ASCII. However, the URI syntax currently only allows a subset of ASCII – about 60 characters. Internationalized Resource Identifiers (IRIs) are sequences of characters from the Universal Character Set that can be mapped to URIs, which means that IRIs can be used instead of URIs where appropriate to identify resources.

The World Wide Web Consortium (W3C) develops protocols and guidelines to maximize 'Web interoperability'. By publishing open (non-proprietary) standards for Web languages and protocols, W3C seeks to avoid market fragmentation and thus Web fragmentation.¹⁴

The Internet Engineering Task Force (IETF) is concerned with the evolution of the Internet architecture and the smooth operation of the Internet through best practices for the Internet Community on the standardization of protocols and procedures. It also addresses the intellectual property rights and copyright issues associated with the standards process.¹⁵

Maintaining a Unified Domain Space

When implementing IDNs, there is a clear need for one domain space, the preservation of compatibility with current domain names, preservation of the uniqueness of the domain name space and the need to ensure that the Internet is not divided into islands.¹⁶ If the domain space is managed by a variety of entities, it will result in an uncoordinated, conflicting and fractured Internet.

As a part of the introduction of IDNs, ICANN has a central function in preventing a breaking up of the domain spaces into regional or local authorities. Otherwise, the Internet will be transformed into islands of information that may very well conflict. For instance, domain space that may be allocated by one region may find that in another domain space managed by an independent domain space authority these web addresses are allocated to other users, owners or organizations.

This would particularly be the case where there are conflicts within language character tables and sets as a result of divergent views and usages. This will not just confuse Internet users but negate the usefulness of the Internet as an efficient tool to target and locate unique web addresses from a global, unified, singular directory. It would threaten the objective of an Internet compatible with globally unique domain names in a universally resolvable public space.

¹⁵ www.ietf.org

¹⁶ These are requirements of the Internet Architecture Board – <http://www.iab.org>

Conclusion

This paper has raised a number of issues and indicated a number of areas where it may be in the best interests of business around the world to provide further input and guidance to interested parties and policy-makers. Potential areas of interest are:

1. Policies regarding mixed IDNs.
2. UDRP reform.
3. Maintenance of a unified domain space.
4. Means of achieving consolidated language tables and character sets.

IDNs are an important next step in ensuring that information through the Internet is accessible to all users around the world.

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

* * * * *

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

Business leaders and experts drawn from the ICC membership establish the key business positions, policies and practices on e-business, information technologies and telecommunications through the EBITT Commission. With members who are users and providers of information technology and electronic services from both developed and developing countries, ICC provides the ideal platform to develop global voluntary rules and best practices for these areas. Dedicated to the expansion of cross-border trade, ICC champions liberalization of telecoms and development of infrastructures that support global online trade. ICC has also led and coordinated the input of business around the world to the World Summit on the Information Society, Geneva 2003, Tunis 2005, and continues this effort in the activities established in the Tunis Agenda.

<http://www.iccwbo.org/policy/ebitt/>

About ICC

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. Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment, e-business, IT and telecoms policy, as well as on vital technical and sectoral subjects. ICC was founded in 1919 and today it groups thousands of member companies and associations from over 130 countries. www.iccwbo.org

Section 6

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



Policy Statement

The impact of Internet content regulation

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

Introduction

Internet content regulations are increasingly prevalent. For example, Reporters Sans Frontieres noted that at least 59 countries impose limits on the freedom of information online. Excessive domestic regulation of Internet content creates significant uncertainties for business operating on this global medium, and has a chilling effect on commercial communication.

The International Chamber of Commerce (ICC) represents global business. ICC's membership includes companies of all sizes, in all sectors, and is geographically diverse. ICC has national committees, groups and direct members in over 130 countries around the world.

This ICC policy statement aims to provide governments, regulatory authorities and courts with a business perspective regarding the effect of content regulations on the Internet and electronic commerce.

Internet content regulation defined:

Internet content regulation refers to any type of legislation by governments or regulatory authorities directed at:

- censoring information and communication on the Internet based on its subject matter, and,
- controlling, or attempting to control, access to Internet sites based on subject matter.

Why is global business concerned about Internet content regulation?

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



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

Business' recommendations to governments

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

1. Allow self-regulation to demonstrate its efficacy --- Filtering, labelling and self-regulation on the Internet should be carefully considered as alternatives to legislation

Self-regulatory mechanisms should be carefully considered as compelling alternatives to legislation, mandatory filtering or additional content restrictions. The market offers a number of rating and labelling services and filtering software, many of which are based on The World Wide Web Consortium's Platform for Internet Content Selection (PICS) that enables labels to be associated with Internet content. A model example is the Internet Content Rating Association (ICRA) that provides free label schemes and filter software.

Business can and does provide users, particularly parents, with the means to filter Internet content while at the same time protecting the rights of adults to express themselves freely. ICC believes that a model, where users can filter out harmful or objectionable content by configuring their software, provides a flexible, balanced and effective self-regulatory mechanism to protect children on the Internet without violating the rights of Internet publishers and other users. Further, the utility of this model should be strengthened by educational programs, aimed at parents, teachers and key personnel in workplaces, to alert users to the availability of such self-regulatory mechanisms.

Any attempt to block communication at some point in the network, including at the Internet Service Provider (ISP), can be bypassed by a variety of means. Thus, regulations that assume an actual ability to block or monitor the flow of information completely are highly inflexible, ineffective and counterproductive.

Transmission of communications through the Internet is highly decentralized and effective control can thus only be reasonably implemented at the two ends (i.e. the host and/or the user) but not in between. Given the availability of encryption, caching and anonymization services¹, attempts to filter between the two extremities are both

¹ Online anonymization service helps users hide their IP address. The service retrieves the pages on the remote server visited and then sends them to the user, so that log files of the remote server will show the IP number of the anonymization service, not the users' IP address.

expensive and largely ineffective. This means that mandatory filtering imposed on Internet service providers and websites is technically and economically unfeasible.

Another fundamental problem involves customer use of anonymization services or proxy servers² abroad. When these services are used, no information about surfed sites is available. Thus, as the table below illustrates, labelling and client-side³ filtering software is more suitable than legislative attempts to limit all access to certain material.

Objective	Possible using self-regulation ?	Possible using legislation ?
Enable adults to protect children from unsuitable material	Yes	No
Enable adults to control their own access to material they do not wish to see	Yes	No
Prevent communication of material which is illegal to possess	No	No

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

- When necessary, regulation should be kept to a minimum and only deal with specific, observed abuses, taking account of existing technologies

Over-regulation of commercial communications is an impediment to trade and, therefore, economic growth. Unnecessary regulation of Internet content creates legal and operational barriers for business, which inevitably has a chilling effect on the integration of the Internet as a tool for business and for promoting economic development. Unrestricted access to information on the Internet plays an important role in business growth in many developing economies, especially in the IT and software industries. Restriction of commercial communications tends to protect domestic or otherwise well-established manufacturers from new competitors. These opportunities should not be jeopardized by unnecessary regulation of the Internet.

- When necessary, laws and regulations should be clear, precise and narrowly tailored

Delivery of Internet content to users involves a number of actors, such as authors, publishers, hosters and other service providers, telecommunication operators, Internet access providers and users, acting within a highly technical and essentially borderless environment. Imprecise laws, regulations and case law create confusion among these Internet actors, which inhibits further development of the Internet.

² When using a proxy server web pages are retrieved by the proxy server rather than by the person actually browsing the Internet. Proxy servers conceal the users' IP-address.

³ Client-side software is software that is installed on the user's computer (the client) as opposed to software that runs on the server (server-side).

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

- a) the domestic and international consequences of the proposed regulation in terms of cost and impact on the development of the Internet and e-commerce;
- b) the underlying technical issues and the precise responsibilities of each of the relevant Internet actors;
- c) an assurance that potential criminal actions are described in clear and objective terminology;
- d) recognition that developing technologies can generate unique observed abuses, relevant regulations should endeavour to be as technology-neutral as possible.

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

4. Legislation should not place additional costs and burdens on business

Where content regulation exists, it is the role of the appropriate law enforcement authority to enforce the law. Legislation and regulation should not place additional costs and burdens on business.

New legislation that would place additional costs and operational burdens on business would risk distorting competition and fetter Internet development.

5. Jurisdiction and applicable law mechanisms should not plague business with the risks of unexpectedly being subjected to laws and judgments in other countries

Internet pages can be viewed anywhere in the world, making all business and consumer users potentially subject to the sometimes conflicting laws and jurisdiction of every country. To avoid this aspect of Internet communications from becoming a deterrent to business and other users of the Internet, authorities should exercise the greatest restraint in imposing their national laws or finding jurisdiction on the sole basis that an Internet page may simply be viewed within its borders. Instead, laws and regulations of a particular country should apply where content is specifically directed to the country in question. For example, does the site solicit, either directly or by its degree of interactive content, an exchange of information with the users in a particular jurisdiction.

6. Provisions dealing with liability should limit the liability of technical service providers and carefully balance the interests of all stakeholders in the electronic environment

The role of access providers and data carriers is to provide other Internet actors with the technical means of implementing Internet communications. Given their role and the high volume of Internet communication, these actors are rarely in a position to control content, and should not, as a general rule, be held liable when content violates applicable



laws and regulations. This is consistent with, for example, the general approach of the EU Electronic Commerce Directive.

The same should be true of hosting providers, except when a hosting provider performs a publishing or editorial function, or otherwise has or should reasonably have, actual knowledge of a violation of applicable laws and regulations. In determining the responsibility of hosting providers, lawmakers should take account of the high volume of content involved and the follow-on costs and impact on competition of implementing envisaged laws and regulation.

Any legislation that deals with the issue of liability should limit the liability of service providers in a manner that balances the interests of all interested parties including copyright owners, communications service providers and users. The US Digital Millenium Copyright Act, EU Copyright Directive and the EU Directive on certain legal aspects of information society services are good examples of an appropriate balance in limiting liability of service providers for copyright infringements of third parties.

Lawmakers are encouraged to consider the effects articulated in this policy statement and engage in critical dialogue with businesses worldwide to ensure the continued growth and vigour of the Internet by providing legal certainties with the least possible burdens and constraints.

Document n° 373-37/1
18 November 2002

Section 7

Policy Statement: ICC Framework for consultation and drafting of Information Compliance obligations

(15 June 2006)



Policy statement

ICC framework for consultation and drafting of Information Compliance obligations

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

Introduction

ICC has been one of the principal voices of international business on data protection, security and associated Information and Communication Technologies (ICTs)-policy issues since the early 1970s. Moreover, ICC has similar substantial experience in dealing with issues of jurisdiction, liability, and corporate governance. This breadth and depth of involvement gives ICC a unique perspective on the evolution of laws and public policy that affect the way companies use and process information and personal data.

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

*Businesses often refer to the legal and regulatory requirements that affect their use of ICT as “information compliance”.
ICC has adopted this term in this policy statement.*

This trend can be ascribed to a number of events and trends since the 1990s: accelerating globalization, corporate scandals, major terrorist attacks (e.g. 9/11), and the maturing of the Internet as a backbone for massive Business-to-Business (B2B) automation. The impact of these requirements is particularly great as they relate to the use of Internet and ICT processes and technologies.

Depending on the way governments impose information compliance requirements, they can either assist businesses in developing better practices or cause severe costs and problems. This policy statement first discusses some of the problems businesses experience in this context, and then suggests legislative principles that governments could consider in order to optimize the effectiveness of information compliance requirements without imposing unreasonable burdens on business.

Problems caused by the current approach to information compliance

Information compliance requirements often impose strict obligations on businesses in areas such as records management/retention, protection of personal data, data confidentiality, integrity and authenticity, authentication and access control. These requirements are being promulgated with great speed and frequency, and usually at national (and/or regional/local/state/provincial) level, at a time when business processes and practices are moving to global applications to service global customers and international markets 24x7x365. This increase in ICT-related requirements from a large number of different regulatory authorities – representing an equally large number of objectives and perspectives – has caused an exponential increase in compliance complexity for businesses that operate globally.

The following are just a few examples of problems arising from information compliance requirements:

- Sarbanes-Oxley “whistleblower” obligations and privacy laws in EU countries: The US Sarbanes-Oxley law requires companies to establish anonymous whistleblower hotlines for employees to make complaints about corporate malfeasance. At the same time, in 2005 the French data protection authority found that these systems violate French data protection law. Guidance from the CNIL has since made it easier for companies to comply with both SOX and French data protection law, but the fundamental conflict between them remains.
- Electronic invoicing in and with the European Union: the EU Invoicing Directive requires taxable persons to guarantee the authenticity and integrity of electronic invoices in transport and storage. The Directive’s broad-brush approach to definitions and the presence of multiple transposition choices for Member States have significantly weakened its harmonizing effect. Businesses – in particular those active in various Member States and smaller national businesses in the EU – face significant problems in just understanding what the actual requirements are, as well as in addressing widely varying national approaches.
- Data retention and privacy requirements: Pharmaceutical companies may be required to consolidate records of adverse event reports in a database in a particular country, while data protection laws restrict the transfer of personal data to that country.
- The US Customs-Trade Partnership Against Terrorism (C-TPAT) includes information compliance requirements for various parties. These requirements are stated broadly, using terms such as “accuracy” and “safeguarding information”. These terms, for which no accepted standard definitions exist today, are not meaningful from an IT systems implementation viewpoint. Little is known about the measures that are considered to be sufficient in this context, and it is unclear how these requirements interact with other IT compliance requirements originating in the US (e.g. FDA rules concerning electronic records) or other countries and regions (e.g. the work on supply chain security within APEC).

These and other information compliance problems create significant challenges to business:

- Obligations frequently differ greatly, and sometimes even conflict, among different regulatory areas and jurisdictions, which can create significant implementation and operational challenges. For instance, companies may be subject to data protection rules in one jurisdiction, which restrict the transfer of personal information across borders, and security requirements in another, which require companies to compile “watch lists” of their global clients.
- The requirements in each country can be difficult to access, and in some cases may even not be set out in writing.
- Often these laws impose serious sanctions; however there is a lack of concrete guidance on how to comply and allowing for companies to avoid such sanctions.
- Businesses increasingly have to understand, monitor and ensure compliance with widely varying ICT-related requirements in numerous different laws in all countries where they are active, as well as in countries that are directly or indirectly affected by their activities.

In reaction to such requirements, businesses have started investing heavily in technologies and services to ensure information compliance. A multitude of product and service vendors are today offering a wide variety of “compliance solutions”. The lack of coordination and predictability resulting from most information compliance requirements often means that companies have no choice but to implement compliance measures on an ad hoc basis; this creates business inefficiencies instead of encouraging businesses to adopt higher standards of information management.

Information compliance requirements can be powerful drivers both for business efficiency and protection of important societal interests. Nevertheless, regulatory authorities and business organizations need to take action to ensure that such requirements become drivers for improved effectiveness, choice, competition, governance, service and quality, and that they not impose disproportionate burdens on business.

Principles for constructive legislative practices for information compliance

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

Proportionate	Information compliance requirements should be proportionate to the regulatory objectives they are meant to serve.
Avoid conflicts	Government cooperation at both the national and international levels should endeavor to assure that business is not faced with conflicting information compliance requirements. When conflicts do arise, authorities should adopt flexible enforcement practices so as to avoid penalizing companies for their inability to comply with such conflicting laws, a problem only public authorities can resolve.
Technology neutral	Any information compliance requirements should be technology-neutral with respect to user choice and stated in terms of functional objectives, rather than in prescribing solutions. Stated objectives should follow internationally-accepted terminology with a defined meaning in the information technology sector.
Future-proof	Any information compliance requirements should be sufficiently flexible to accommodate future changes in technology which will undoubtedly occur, but which cannot be fully anticipated.
Standards-informed but not standards-specific	Government agencies that plan to introduce information compliance requirements should seek business advice on commonly-used industry standards and reference frameworks, and should avoid mandating specific standards. Standards used in compliance requirements should be market-driven, consensus-based, developed in an open process with participation from all affected industries.
Mindful of economic impact	Governments should be mindful of the cost and potential additional liabilities associated with implementing information compliance policies and practices and should analyze the economic and social impact of these measures in the pre-existing regulatory environment before imposing information compliance requirements.
Clear	Information compliance requirements and applicable sanctions for non-compliance should be expressed unambiguously.

Non-discriminatory	Governments should avoid operational, financial or other direct involvement in the supply of compliance products or services. If such involvement is nevertheless a reality, information compliance requirements in laws should not favor the use of such products or services over other information compliance products and services.
Enforcement	Enforcement of information compliance requirements in law should be non-discriminatory and allow reasonable time for businesses to remedy shortcomings once identified.
Flexible	Governments should recognize that private sector compliance may require different approaches depending on factors such as a company's sector(s) of activity, connectivity, geographic spread, size, as well as economic or strategic importance.
Pro-competitive	Compliance requirements should avoid creating competitive disadvantages within and across national and sectoral borders.
Pro-trade	Information compliance requirements in laws should not create or maintain obstacles to international trade, including the cross-border delivery and use of information compliance products and services. Specific national information compliance requirements and standards can cause entry barriers for foreign products or services providers, which in addition to creating obstacles to trade can negatively affect the competitiveness of local businesses.
Resources and preparedness	Governments should ensure that before creating information compliance requirements, information and support services are in place to respond to reasonable business questions about the requirements and their practical implications. Governments should also ensure that, before information compliance requirements become effective, enforcement officers have the training and means required to ensure effective, neutral and consistent enforcement, and that enforcement decisions are published in a timely manner.
Period of grace and independent appeal	Governments should offer companies a period in which any shortcomings in systems that are deemed to be non-compliant by regulatory authorities can be remedied in order to avoid sanctions. Final compliance decisions by regulatory authorities should be appealable to an independent body with sufficient power and means to decide and effectively enforce decisions in a reasonable timeframe.



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

Business leaders and experts drawn from the ICC membership establish the key business positions, policies and practices on e-business, information technologies and telecommunications through the EBITT Commission. With members who are users and providers of information technology and electronic services from both developed and developing countries, ICC provides the ideal platform to develop global voluntary rules and best practices for these areas. Dedicated to the expansion of cross-border trade, ICC champions liberalization of telecoms and development of infrastructures that support global online trade. ICC has also led and coordinated the input of business around the world to the World Summit on the Information Society, Geneva 2003, Tunis 2005, and continues this effort in the activities established in the Tunis Agenda.

<http://www.iccwbo.org/policy/ebitt/>

About ICC

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. ICC promotes an open international trade and investment system and the market economy. Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment, e-business, IT and telecoms policy, as well as on vital technical and sectoral subjects. ICC was founded in 1919 and today it groups thousands of member companies and associations from over 130 countries.

www.iccwbo.org

Document N° 373/472
15 June 2006 AH/MvdL/dfc

Section 8

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



Policy statement

Open Source Software

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

Introduction

ICC recognizes that “open source” software has become a topic of great interest in the press and among policymakers. Open source software –as a software development and licensing model – is an emerging business reality that deserves thoughtful consideration. It is appropriate to address this subject in a balanced way and to look at the practical, pragmatic issues surrounding the emergence of this software development model in the marketplace, and the public policy implications.

“Open Source” Software

Generally speaking, open source software (OSS) refers to software for which the underlying “source” code (the programme text written in a programming language, such as C and C++, that is understandable to humans) is available for inspection and modification by anyone interested in doing so. This contrasts with proprietary software, the source code for which is often not made available to third parties. The term “open source,” coined in the late 1990s, is often applied in two distinct ways: (1) to a software programme licensed under particular terms and (2) to a software development model.

Licensing considerations:

Open source software may be distributed under a number of different software-licenses.¹ For example, open source software may be licensed under permissive terms that allow third parties to modify or incorporate the software into a new programme without requiring that the new or modified programme be licensed under the same terms. An example is software subject to the BSD license.² On the other hand, open source may also be licensed under terms that set forth specific rules for its distribution, reuse, or modification. A common example is the GNU General Public License (“GPL”). The GPL requires licensees of a GPL-covered work who distribute the object code version of the work to also make the source code version of the work available to anyone who receives the object code version that they distribute. This requirement that source

¹ A useful table outlining the terms and features of ten different “popular or significant” open source licenses may be found at M. Fink, *The Business and Economics of Linux and Open Source* 42-25 (Prentice Hall PTR 2003)

² The BSD or Berkeley Software Distribution license only requires that re-distributions of code covered under it identify the original copyright holder(s) and pass through a disclaimer in the form of an “as is” warranty. See BSD license, <http://www.opensource.org/licenses/bsd-license.php> (last visited August 13, 2004)

code be made available also applies to the source code for works that a licensee derives from a GPL-covered work. All GPL-covered works, including their derivatives, may only be distributed under the GPL. The GPL does not require that source code be made available if there is no distribution to a third party. However, not all open source software is covered by the GPL and there are in fact several open source licenses with less restrictive terms than the GPL. The Open Source Initiative is the organization that determines whether or not a given license meets the requirements to be deemed an “open source license.” There are presently over 50 such licenses listed on the OSI web site.³

The term “open source” should not be confused with the term “public domain.” Authors of software that is in the public domain have no right under copyright law to impose restrictions on the copying, distribution, modification, or other use of the software. Authors of open source software, by contrast, do exert copyright control over their software and may be very specific in their licensing requirements for the distribution, reuse or modification of their open source code. They do not simply make the code available to the public without restriction, as would be the case if the code were in the public domain. These licenses are quite different from works said to be in the “public domain” or commonly referred to as “freeware” or “shareware.” The term “open source” also does not equate with “free” in the sense of price or cost of ownership.

Characteristics of the development model:

Open source development projects are typically made up of a diverse group, ranging from employees of an enterprise whose job it is to participate in a particular open source development project to others, often in the education and research communities, who are interested in the development of the code for a variety of reasons. Often the project leader adopts a role of finalizing the programme version and accepting modifications into a future version of the programme, so not all changes are automatically incorporated; they are simply made available for review by the project members and other participating in the open source community. Because the source code is viewable by all, the underlying technology can be used by developers outside the original community in other ways, thus offering flexibility for future software needs. More recently, the establishment of the Open Source Development Laboratory by a consortium of technology companies has brought commercial practices more often associated with proprietary software to some major open source development projects such as the Linux operating system. The Apache Software Foundation and the Eclipse Software Foundation are also good examples of more formal open source development models that receive support from a number of technology companies and employ rigorous development and review procedures.

³ See <http://www.opensource.org/licenses/>.

Open Source Software in the marketplace

The software marketplace is large and complex. According to IDC, the packaged software industry is a \$190 billion industry that employs millions of people. This number does not include the vast value of software that is created within an organization for its internal use. Open source software is a significant and rapidly growing part of the software marketplace. Examples of Open source programmes include the operating system Linux, the Web server Apache, development tools like Eclipse, Perl and PHP, MySQL, a relational database system and the jBoss application server. Today there are an estimated 2.6 million Web and file servers running GNU/Linux. The Apache HTTP Server Project, an effort to develop and maintain an open-source HTTP server software product that can run on various operating systems, holds a leading share of the market⁴. Users include some of the largest and most prominent companies in the world.

Questions to consider when procuring software

Procurement leaders in government and industry should consider many factors when acquiring software that apply regardless of the licensing model. In evaluating or choosing a software model, many questions may be addressed, including:

- a) How does the functionality of any particular software address the relevant business needs?
- b) What is the total cost of customizing, implementing, managing, improving and maintaining the software over its useful life?
- c) What kind of services are provided, or what local services are available to maintain, modify or customize programme source code?
- d) How interoperable is the software with other programmes?
- e) How secure is the software and what resources (vendor or otherwise) are available to respond to attacks?
- f) Has the software completed direct or third party security evaluations of the product and the development process?
- g) What is the stability, utility and assurance related to the rights transferred in the software?

Each software license has distinct elements; there can be advantages and disadvantages to both open source and proprietary software, depending on the individual customer environment in which the software is to be deployed. Neither model possesses exclusive benefits. Rather, they reflect the rich diversity that exists in the software marketplace and purchasers need to decide on a case-by-case basis which combination of factors and characteristics best suit their needs.

Companies can participate in the market with both models for different products at the same time, e.g., for different product lines. Customers, as well, can decide freely which software

⁴ Gartner Group prediction. Business Week, January 12, 2004. ⁴ In a July 2004 Netcraft survey incorporating roughly 57 million Web sites, Apache ranked as the market share leader, with 69.5% market share and 16,774,339 active servers. According to Netcraft, the number of sites deploying Apache has risen to about 35 million. It has held the market leader position for about 10 years. See http://news.netcraft.com/archives/2004/07/01/july_2004_web_server_survey.html (last visited August 13, 2004)

product they prefer. It is expected that in the future, players in the marketplace will act in both models and use each of the models as appropriate.

Moreover, as open source software becomes more commercial, and as commercial software becomes more open, the above factors become less distinct. Instead, procurement leaders should evaluate software on a product-by-product basis relative to these factors and policy leaders should support this evolution by not looking solely at the development and licensing models as they set software public policy.

Open standards and Open Source Software

“Open standards” are publicly available technical specifications. While there is no universally accepted definition of the term, open standards are regularly developed, maintained, approved, or ratified by consensus and published without restriction, in a market-driven standards-setting organization that is open to all interested and qualified participants. Standards can also develop by consensus in the marketplace.

Standards setting organizations (SSOs) independently create their rules for participation and use, which may include obligations for participants to commit to license essential patent claims in their contributions to the standard. If the standard includes technology covered by patent claims (incorporated with the permission of the rights holder), it may be licensed on fair, reasonable and non-discriminatory terms, with or without a royalty or fee, depending on the rules of the particular standardization body. On rare occasions, dissemination of the standard may also be accompanied by licensing terms that require the licensee to license any improvements it makes to the standard to other licensees, including the licensor, in order to maintain the specification’s quality as a uniform “standard” available to all market participants. However, one of the pro-competitive aspects of standardization is the fact that entities can provide their own unique value by adding technology on top of the standard to differentiate their products and provide competitive value to their customers.

“Open standards” are not the same as “open source software. Whether a specific standard qualifies as “open” has nothing to do with the development model or licensing terms associated with software that implements the standard.⁵ Open standards (technical specifications) may be implemented by all types of software. Open standards do not inherently favor one model of software development or licensing over another, but instead, as technical specifications, document requirements that must be met so that products that implement the standard can exchange and use information with other products that also implement the standard.⁶ Thus

⁵ “Open source standards” do exist. For example, a group called the “Free Standards Group” (www.freestandards.org (last visited August 13, 2004)) is engaged in a number of standards projects, such as developing standards and test suites to allow/enhance portability of applications across Linux distributions and different numbered releases. Sometimes, however, it appears simply that the terms “open source software” and “open standards” are confused because both contain the word “open.”

⁶ An example may be helpful. HTML is an open standard. Mozilla, a product of Netscape, is an open source web browser software programme that complies with the HTML standard. Internet Explorer, a web browser supplied by Microsoft with proprietary code, also complies with HTML standards.

governmental support for open standards provides no justification for favoring one software developing or licensing model over others.

Governments can play an important role in advancing open standards. That said, governments should avoid policies that inadvertently discourage the development and adoption of broad-based open standards, either by mandating standards themselves (which can freeze innovation) or mandating those that have not achieved broad industry support, or by reducing the economic incentives to participate in standards-setting processes.

Public policy implications of Open Source Software

Procurement preferences

Since the late 1990s, some governments at the sub-national and national levels have considered changing their public sector procurement laws to give preference to open source software by either creating barriers to the acquisition of commercial software (or preferences for acquisition of open source software) or making the purchase of commercial software by government procurement authorities' outright illegal. ICC opposes government procurement preferences and mandates that favor one form of software development or licensing over others. Governments, like all potential and existing customers, should choose software on a technology-neutral and vendor-neutral basis, examining the merits of the technology based upon the performance factors stated above. As a general rule, governments should not discriminate against or ban the procurement of software based on its licensing or development model. Such preferential policies prevent public authorities from effectively weighing all relevant factors in their procurement decisions.

Funding for research

Publicly funded basic research in software is an important source of innovation in both commercial and open source communities. It enriches the commons of knowledge, helps train the next generation of technology leaders and provides raw material that can be further developed into commercial products.

Permissive open source licensing can facilitate uptake of publicly funded research by developers working in both communities under all licensing models. Governments should provide public funding for basic research in software where possible, and to maximize the return on public funding, apply permissive open source licensing to serve the dual purpose of expanding the commons while allowing ongoing development in both communities.

Intellectual property concerns

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

Conclusion

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

About ICC

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. ICC promotes an open international trade and investment system and the market economy. Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment, e-business, IT and telecoms policy, as well as on vital technical and sectoral subjects. ICC was founded in 1919 and today it groups thousands of member companies and associations from over 130 countries.

Document N°373/466

27 October 2005 AH/MvdL/dfc

Section 9

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



Policy Statement

Deploying the next generation Internet:

ICC statement on the introduction of IPv6

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

Introduction

ICC is uniquely positioned to encourage business and governments around the world to promote the benefits of a smooth transition from IPv4 to IPv6. Representing Internet users and service providers globally, ICC endorses the progressive introduction by business of IPv6 and advocates for increased awareness among business and governments on the benefits of IPv6.

IPv6 is the acronym for Internet Protocol version 6. IPv6 is the 'next generation' Internet Protocol designed by the Internet Engineering Task Force (www.ietf.org) to coexist with and ultimately replace the current version Internet Protocol, IP version 4 ("IPv4"). Internet Protocol (IP) is a set of technical rules governing how information travels around and can be found on the Internet. IP lets different computers communicate with each other over the communications networks that comprise the Internet.

Every network interface on the Internet has a unique IP number. These numbers are called IP addresses and they can be typed directly into a browser or linked to a named web address such as www.yourcompany.com

IPv4

Today, the Internet relies mostly on IPv4, the version of the Internet Protocol that was specified nearly twenty years ago. IPv4 is still robust, but it supports a relatively limited number of IP numbers. Several factors are driving increased demand for IP numbers:

- The number of Internet users increases significantly each year, creating more and more demand for IP addresses. While IPv4 allows for four billion computers on the whole network, IPv6 allows for upwards of 35 trillion interconnected networks.¹ As developing countries work towards bridging the digital divide and increasing their access and connectivity to the Internet, the demand for IP addresses will continue to grow.

¹ Source: 'IBM Vision for IPv6 in the era of e-business on demand', July 2003

- Future Internet application developments such as wireless communications, mobile computing and next generation telephony will further increase demand for IP addresses.
- The increasing popularity of mobile devices such as mobile phones, portable devices and laptops will also greatly drive demand for IP addresses. Cars and household appliances may also be assigned IP numbers as they too become communications devices.

The availability of IP addresses using IPv4 has been increased through the deployment of dynamic address translation. Furthermore, the integration of IPv6 and the coexistence of IPv6 and IPv4 will be facilitated since new technologies and applications using IPv6 may actually “free-up” some IPv4 addresses as earlier technologies and applications are replaced. The transition from an IPv4-only environment, which began a number of years ago, may continue for an undetermined period of time.

The benefits of IPv6

The new version of the Internet Protocol, IPv6, will enable new capabilities beyond IPv4, including providing greatly increased availability of IP addresses.

The benefits of IPv6 include:

- The number of IP addresses available with IPv6 is enormous - 3.4×10^{38} (i.e. 10 to the power of 38) – and will not be exhausted in the foreseeable future
- IPv6 improves the efficiency of the Internet. Simplified packet header information allows for more straightforward and efficient routing of Internet packets. Shorter routing tables are possible because most Internet service providers can receive address space in adjacent blocks, offering greater convenience to their clients and also allowing for a more efficient structure in the Internet’s core routing tables.
- IPv6 creates opportunities for new types of services that prioritize Internet traffic flows. It is ‘auto-configurable’, meaning devices like laptops, PDAs and mobile phones can be given their own unique IP addresses easily and without delay. This will simplify the installation and maintenance of home, vehicle and small office networks.
- IPv6 improves security by facilitating network-level security. It has security services at the IP-layer as a ‘native’ feature (i.e. IPSec includes the following capabilities: data origin authentication, rejection of replayed packets, and encryption). Also, allowing each communications device to have its own unique IP number facilitates ‘end-to-end security’, meaning that an entire communication session can be conducted securely rather than just the parts that use a virtual private network.
- IPv6 provides the basis for continued technical innovation in communications technologies.

Challenges in IPv6 deployment

As with the upgrade of any network, computer or related technology, deploying IPv6 generates costs, interoperability and resource issues for Internet stakeholders.

- Network routing and related Internet architecture equipment will need to be upgraded or modified to accommodate IPv6 128 bit addressing (as compared to 32 bit for IPv4).
- Although the number of IPv6-enabled Internet applications is constantly increasing, not all applications are presently engineered to work in an IPv6 environment.
- Having both protocols coexist in Internet architecture as IPv6 continues to be deployed generates integration and interoperability costs and challenges.

These issues may require Internet stakeholders to prioritize and concentrate their continued IPv6 implementation where it is most needed and will have the greatest benefit.

The path forward

It is in the interests of all Internet users that the Internet continue to evolve and thrive. IPv6 is an important step in this regard.

The integration of IPv6 does not have a hard deadline like, for example, the system changes for Y2K did. IPv6 will coexist with IPv4 for a number of years. However, it is still essential that IPv6 deployment be prioritized to ensure that it occurs and that interworking of IPv6 and IPv4 be accommodated.

Governments should not mandate IPv6 transition. Rather, this transition will occur in gradual stages that allow consumers, business and governments to adopt IPv6. Businesses and governments each have an important role to play in ensuring a smooth and timely evolution with IPv6.

Recommended business actions

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

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

- Business must recognize that the security and stability of the existing network is an essential requirement in the transition period when IPv4 and IPv6 will coexist.
- Business should continue its efforts to improve government and consumer awareness of the importance and benefits of IPv6, for example, through initiatives such as the IPv6 Forum (<http://www.ipv6forum.org/>), a consortium of vendors, which organizes information events around the world to increase awareness and promote the adoption of IPv6.
- Business should continue to provide expert input into the technical coordination bodies responsible for developing and overseeing IP and its related protocols, particularly the Internet Engineering Task Force (IETF). This input will help ensure that as new technologies develop, they are compatible with and take advantage of IPv6.

Recommended government actions

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

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

- Governments should work to increase awareness of IPv6 and its benefits.
- Governments should support the integration of IPv6 and the coexistence of IPv4 and IPv6 to address user needs, including planning initiatives.
- Governments should avoid mandated standards or legal requirements, and ensure that their policies on IPv6 implementation do not impose deadlines.
- Governments should continue to promote technology neutrality and choice, allowing Internet stakeholders to use new and existing technologies and applications of their choice.
- Governments should support relevant research and development to ensure a smooth and effective integration of IPv6 and associated technologies.

Conclusion

The deployment of IPv6 requires a significant planning and awareness-raising effort by business and governments in the medium term. The benefits of the introduction of IPv6 will accrue to all Internet users well into the future. ICC encourages business and governments to maximize and coordinate their efforts so that all Internet users will benefit from the increased efficiency and opportunities IPv6 offers.

Document N° 373-31/7

2 December 2004 MvdL/MF/dfc

Section 10

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

(5 July 2006)



Department of Policy and Business Practices

Commission on E-Business, IT & Telecoms

Task Force on Privacy and Protection of Personal Data

**Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data outside the EU
(to be used in all EU Member States)**

Introduction and Instructions

The EU Data Protection Directive 95/46/EC allows personal data to be transferred outside the EU only when the transfer provides an “adequate level of protection” for the data. Binding corporate rules (BCRs) are one of the ways in which such an “adequate level of protection” may be demonstrated.

The use of BCRs to provide a legal basis for international data transfers from the EU requires the approval of the European data protection authorities (DPAs) from whose countries the data are to be transferred. The following form is to be filled out by a group of companies seeking approval of BCRs. The form is based on papers issued by the Article 29 Working Party of European data protection authorities (the “Working Party”). It is being submitted to the Working Party in the hope that it will prove useful in furthering acceptance of BCRs as a legal basis for the transfer of personal data outside the EU.

General Instructions

Only a single copy of the form need be filled out and submitted; this form may be used in all EU Member States.

Please fill out all entries and submit the form to the lead DPA as determined below. You may attach additional pages or annexes if there is insufficient space to complete your responses.

Please indicate any responses or materials that may be commercially sensitive and should be kept confidential.

The footnotes indicate the relevant provisions of the Working Party papers WP 74 and WP 108, which contain further clarification of the questions.

The form may be filled out based on the common criteria for approval identified in the Working Party papers.

Once you have submitted the form, the lead DPA will contact other DPAs from whom you are seeking approval, and will get back to you with any questions or requests for further information.

The complete 33 page form can be easily downloaded at:
http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/Standard_Application_for_Approval_of_BCRs.pdf

Section 11
ICC Tools for E Business



International Chamber of Commerce

The world business organization

Department of Policy and Business Practices

ICC Tools for E Business

The following Tools for E Business have been produced by ICC:

- Information security assurance for executives
- Securing your business
- Privacy toolkit
- Resolving disputes on line
- Procuring ICTs
- Telecoms Liberalization

These toolkits are also available on our website:

<http://www.iccwbo.org/policy/ebitt/id2132/index.html>

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

October 2006 AH /apn

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.

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



International Chamber of Commerce

The world business organization

38, Cours Albert 1er, 75008 Paris, France

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

Website www.iccwbo.org E-mail icc@iccwbo.org