International Chamber of Commerce
The world business organization

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.

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

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