International Chamber of Commerce
The world business organization

Policy and Business Practices

International Chamber of Commerce (ICC) Comments on EU Directive: 95/46/EC

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS
'A comprehensive approach on personal data protection in the European Union'

The process related to the review of Directive 95/46/EC is critically important in today's world of national, regional and global information flows. The Directive and its national implementations form the basis for exchanges of personal data both within the EU region and globally. We thank the Commission for the opportunity to provide these responsive comments and look forward to working constructively with the Commission and the broader stakeholder community in this process.

Our comments go to both the substantive recommendations of the Commission Communication as well as to the illustrative examples used. The comments related to illustrative examples are provided to add further context to issues that are important to consider as the Commission contemplates revisions to the Directive that may impact those examples in deployment. We also believe that this Commission Communication helps shape the context of the policy debate going forward and wanted to ensure that it was as reflective as possible of both the concerns and potential benefits related to new applications of technology and emerging business models.

In addition to our comments in response to the Consultation, we also attach the "ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data of December 2009" which, while not directed specifically to this Consultation provides relevant business views on the current legal framework protecting the fundamental rights of data protection and ways it could be improved.

We are gratified that the Communication highlights and reaffirms the importance and continued validity of the dual objectives of the Directive EC 95/46 ("Directive") – the protection of privacy and free flows of information that are integral to the creation of an Internal Market. We also concur that globalization, new technologies and the increased scale and immediacy of information provide the context for evaluation of the Directive.

Where the Communication sets forth concerns to be addressed in the review, we believe that greater precision may be needed in the examples provided to prevent improper conclusions being drawn from partial information. We are confident that this issue arose from a desire to be expedient in drafting and to assure that focus was placed on the

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

greatest concerns of citizens and authorities. It must be recognized, however, that too narrow a focus on only the protection of privacy may undercut the ability to deliver on the promise of a vibrant and competitive Internal Market of information services by not providing the right context for optimizing both objectives. We fully believe in and support finding ways to meet the needs of citizens and privacy authorities. However, we also believe that it is critical to, at the same time, enable the information flows needed to assure a vibrant and globally competitive market of information services in Europe, as well as globally. Both objectives should be optimized.

An illustrative example of the above concern may be of use. The Communication correctly highlights that:

> *'Cloud computing' … could also pose challenges to data protection, as it may involve the loss of individuals' control over their potentially sensitive information when they store their data with programs hosted on someone else's hardware.*

In addition, it does not recognize the different types of cloud services/applications that may be characterized by different service provider-customer relationships that impact privacy and security considerations. Because this Consultation will elicit opinions from a broad range of stakeholders, some of whom may have limited technical expertise, we are always concerned that information provided in only partial context may create a desire for ill-advised controls not tailored to preventing the real risk/threat at issue, but rather an incorrect perception of that threat. While this may seem to be quibbling, we are mindful of the importance of the review of the Directive and the critical role of this consultation.

Another example would be in the context of less detectable information collection:

> *For example, the use of sophisticated tools allows economic operators to better target individuals thanks to the monitoring of their behaviour.*

Again, the clause raises a legitimate concern related to the potential for misuse of this information, but does not highlight the potential for consumers to benefit from services based on the information they provide where they are also provided clear notice, effective choices and proper oversight.

Each of these tools has the potential for enhancing risks to privacy if misapplied or misused, but also has the potential to provide growth and societal benefit through innovative services. We are in no way suggesting that discussion of risks should be minimized or even of greater focus, but we do request that proper recognition of

potential benefit from innovative services and technologies also be referenced to correctly inform the context within which the revision of the Directive will occur.

We appreciate that the Consultation has prominently highlighted the need for improved harmonization within the Internal Market and consideration of improved mechanisms related to globalization and international data transfers. These are critically important elements of the review in light of today's more global commerce that is supported by information flows which are the currency of the digital economy. We would also suggest a focus on efficiency of regulation to ensure that regulation is effective without being unduly burdensome. We recognize that these themes are addressed later in the Consultation, but believe that they should also be highlighted in this part of the paper as they complement the sections discussed above and also inform the reference to more effective enforcement of data protection regulation.

We appreciate the conclusion drawn from this analysis of concerns/objectives but believe that the phrasing may be subject to misinterpretation.

> *The above challenges require the EU to develop a comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected within the EU and beyond.*

The ICC has long argued that extraterritorial application of laws frequently subjects companies to conflicting or overlapping legal requirements, fosters unpredictability, increases the risks involved in commercial activities, exposes companies to overly burdensome litigation in foreign jurisdictions, and inflates legal and other transaction costs.[1] The Directive has always been viewed as applying to personal data relating to EU citizens within the EU and where transferred. We believe that the above clause is referring to that concept. Some may misinterpret the language to suggest a wider impact on national laws outside of the EU. While we are aware that the EU has always welcomed countries to develop legislative frameworks consistent with the Directive there has never been an intention of imposing such requirements, except as to EU data. Therefore in the upcoming legislative review, we would suggest that any provisions within this context are drafted with more bounded statements of the objective to ensure that the intent is correctly understood and reflect ICC's caution against extraterritoriality.

[1] See ICC Policy Statement Extraterritoriality and Business
http://www.iccwbo.org/uploadedFiles/ICC/policy/trade/Statements/103-33%205%20Final.pdf

Section 2

2.1.1. Ensuring appropriate protection for individuals in all circumstances:
We completely understand the focus of this section to be on individuals and clearly on the objective protection of their rights. That being said, the document should remain consistent in highlighting that this is "*an*" as opposed to "*the*" objective of the Directive.

We appreciate that the Consultation has taken into account the complexity of the definition of personal data in terms of needed flexibility of application as well as the need for certainty. We fully support the conclusion that:

> *The Commission will consider how to ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms and the objective of ensuring the free circulation of personal data within the internal market.*

We would like to stress again what we have indicated in the "ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data of December 2009": When defining "personal data," account should be taken of whether the data processor or controller has a realistic possibility of linking data to a given individual. There are many situations where an organization has no practical ability to actually identify an individual, and thus there is no need to consider data processed in such circumstances to be "personal data."

2.1.2 Increasing Transparency for data subjects:
We concur with the concerns highlighted regarding transparency and notice, but wonder if greater clarity can be provided related to the proposed action. A general principle of transparency may lend itself to a variety of interpretations. While we support the need for improved transparency where confusion may exist, we are concerned that some efforts to provide granular information related to complex processes or value chains may actually have a contrary effect. Individuals need useful information, which in many cases may accurately summarize processes or systems. Too much information may improperly burden the data subject in terms of both volume and technical nature of the information. To that end we support the use of plain language where possible, but also need assurance that useful expression of policies in plain language can meet the detailed legal requirements of disclosure. Lastly, we see a benefit for model notices, but would like to ensure that they are conceived as model frameworks and not fixed statements which preclude the needed flexibility for tailored description of company practices

We are equally supportive of the Communication's consideration of data breach as a topic. Companies with operations in the United States (USA) have had substantial

experience in the operation of a variety of such practices among the states of the United States. While all have seen some beneficial impact from breach notification we have also seen the negative impact of over-notification. Unfortunately, a proliferation of notification may lead individuals to start to ignore as opposed to act upon them. That is why in many US states, Canada and the EU (related to the e-privacy Directive) regulations related to breach notification enabled some flexibility of application and triage based on a harms or adverse effect principle. In other words using the potential impact of the breach including the type of information and circumstances of loss or access as factors in the entity's determination of what if any notification is appropriate and to whom. Methods of notification must also be considered to assure that practices do not create conflicting notification requirements across jurisdictions.

2.1.3 Enhancing Control over one's own data:

Business has been working to improve the ability of data subjects to appropriately control their data. The word appropriate is important as the control of data is not a right, but rather a way in which rights are enforced. As such mechanisms to enhance the control of data are not unlimited. For example, an individual cannot prevent the use of certain financial information being considered for a loan. Control of data is also limited by the realities of networks and technology.

The breadth of the right to be forgotten has unfortunately been taken to a less achievable goal of impacting information on the net wherever located. For example, if a user posts information in a way that is accessible to the general public via a social network, the service provider has no technical ability to delete information that may have been copied or forwarded to resources beyond their control.

It should be recalled that, as foreseen in the current EU legal framework, all parties who deal with personal information have related obligations of compliance, including not maintaining information beyond a time reasonably related to the purpose of collection and sharing on where derogation or consent exists. More specifically, a form of the right to be forgotten is already encompassed of Art. 12 of Directive 95/46/EC in that it provides individuals with the right to request the rectification, blocking or erasure of personal data. Therefore, this issue is rather a question of proper enforcement of existing legal obligations. The rhetoric today that seems to provoke a rather philosophical debate on a new "right to be forgotten" in the online (and offline?) world, does not seem to be considering practical difficulties and unintended consequences related e.g. to metadata and back-up systems, data retention requirements and other technological, financial and legal complexities.

Portability creates a more complex set of issues. While all would agree that "lock in" is undesirable and that open standards facilitating the portability of information across competitive services are preferred, it is very difficult to require that information from one application or service be useful in another application or service. One major issue is that applications often have significantly different functions, uses and formats of information limiting potential utility of portability. In many cases this is driven by product differentiation and tailoring products to emerging or more specialized market needs. We are also concerned about the implications on innovation of regulation that is overly prescriptive and specifies detailed formats or functionality implementations. While portability may be an objective to the extent it can be accomplished through open standards, and portability implications or methods may be an element of disclosure, we do not think that it can be a mandated solution.

Furthermore, the issue of data portability is also addressed by Article 12 of Directive 95/46/EC in that individuals have the right of access to their personal data and any information on the processing thereof. We do not think that further regulation is needed in this area.

2.1.5 Ensuring informed and free consent:

We appreciate that consent has become more complex over time and that the clarity of consent may need improvement. We are also not opposed to strengthening consent where needed, but do not believe that the examples preceding the recommendation provided clear examples of weak consent. Better examples may help clarify the difference between weak and unclear consent in future guidance. Furthermore, the reality of interactions (online or otherwise) is that they do not provide the opportunity to meet all of the individuals wishes or peculiarities related to consent. The current state of the art with respect to online interactions, through social media for example, allows for systematic selections of preferences and graduated choices which allow some flexibility in what and how personal data is collected, used, retained or shared.

2.1.7 Making remedies and sanctions more effective:

When considering the effectiveness of enforcement, we understand and support the need to enable authorities to engage in consistent and effective enforcement. That being said, our experience of class or reprehensive actions is not positive. These class actions are subject to abuse and serve to dramatically increase the cost of doing business without commensurate improvement in the effective enforcement of privacy. Many of these actions are related to administrative and technical failures as opposed to intentional and flagrant misuse of information. In fact, across all privacy authorities and attempts to enhance enforcement, there needs to be a greater focus on the true bad actors that

intentionally attempt to breach and exploit information, not just the organizations that they prey upon.

2.2 Enhancing the internal market dimension

We are very gratified by the Communication's inclusion of the need for greater harmonization and clarity of application of the Directive within the EU as well as the need to reduce administrative burdens. Those sections are followed by consideration of clarification of applicable law in transborder data flows, enhancing the responsibility of controllers and the consideration of self regulatory initiatives. We believe that all of these topics are directly related in the evolving data protection ecosystem.

In discussions related to the review of the Directive the focus has been on effective regulation. We strongly support this concept as we believe that a number of existing administrative procedures do not significantly contribute to effective data protection in their current form; these include both registrations related to processing and prior notification of cross-border data transfers. In both of these cases both the purpose and procedure need to be considered. To be clear, we are not advocating for the reduction of protection, but rather a consideration of the means of compliance to ensure that burdens are tied to effective outcomes. When the Directive was first implemented, the technical realities of EDI (electronic data interchange) and discrete nature of information flows made the registration of processing and notification of transfers more relevant and meaningful. Today's more global and commingled flows of data make those vestigial procedures less relevant to effective regulation and compliance. Those resources devoted to administrative review would be better used in targeting bad actors for enforcement.

Further, the harmonizing effect of the EU data protection directive should be more rigorous, meaning that administrative measures in the different member states should be applied consistently across the EU as currently a divergent trend can be observed. In considering the benefits of harmonization, attention should also be paid to impacts of divergent sectoral requirements, such as money laundering rules, on the governance of personal data.

2.2.5 Encouraging self-regulatory initiatives and exploring EU certification schemes:

We are also supportive of the exploration of how private sector third parties may play a role in supporting authentication, enforcement, compliance and potentially other functions. They assist entities dealing with user data and provide useful leverage for enforcement and oversight functions of data protection authorities. In the USA and Asia Pacific there has been experience in the use of such third party accountability and authentication agents and how they work in conjunction with enforcement authorities that may be relevant. It is important to note that we believe that any such initiatives should not impose redundant enforcement procedures vis-à-vis enforcement authorities.

The Communication also mentions their potential role in certification schemes. We are interested in better understanding the intention behind this concept. There is broad experience related to certification ranging from effective processes to assure a threshold of compliance to more detailed and burdensome investigations that may cause both delay and cost that is not correlated to the compliance objective. The former adds certainty assuming that it is properly recognized, while the latter often serves as a tax with no commensurate enhancement of compliance that can serve to retard innovation.

We are also supportive of the objective of privacy-by-design, and the use of privacy tools, such as Privacy Impact Assessments (PIAs). Indeed, legitimate businesses today are already developing privacy-by-design processes including risk assessments such as PIAs to more informal internal controls or the appointment of privacy officers- we must stress the need to apply both tools and concepts in a flexible and tailored manner. These are not one-size-fits-all exercises. They need to be flexible and adapted for organizations to effectively address user privacy requirements while recognizing infrastructure, physical, human and technical aspects, and taking into account the use and nature of information, including special sensitivities, as well as applicable policies.
In this respect we believe the communication rightly endorses the *objective* of privacy-by-design and other privacy tools but we would caution that the upcoming legislative review should not dictate or over specify how the design objectives are to be met or the details of operational processes.

2.4 The global dimension of data protection:

It is important to consider the certainty related to global transfers and interoperability across divergent systems. Adequacy has been the traditional way of establishing permissibility of cross-border transfers from the EU. In today's world information flows are more global and less defined by point-to-point communications. Moreover, The current set of rules for international data transfer does not allow for a reasonable handling of data within a corporate group which leads to numerous problems. To monitor data flow within corporate groups various frame-agreements and contracts regarding commissioned data processing are necessary. These contracts need to be administered and controlled, consuming significant financial and human resources. With the above in mind, we believe it is essential to consider how to apply the concepts that underpin adequacy more globally. Where companies fall under consistent corporate governance a comprehensive data processing must be feasible according to the group's organisation. Binding Corporate Rules present an important development in this area of global compliance approaches to information flows. Although the complexity and cost of the approval process has improved over time, they are still sufficiently burdensome to discourage many companies from undertaking the effort to invest the considerable resources necessary. The solution is evolving and previously prohibitive administrative procedures are being streamlined to better enable mutual recognition across member

countries. Further progress in this regard to confirm an EU-wide one-stop-shop would significantly enhance the attractiveness of this option. Accountability is a concept also being considered as a principle on which to base global solutions. It has both domestic and cross border elements to ensure that data protection is considered in a comprehensive and demonstrable fashion. Accountability, depending on its development, could provide enhanced effectiveness, but may also increase burdens related to compliance if it is introduced in the legal framework as an additional requirement rather than as an underlying principle. In considering the data protection and compliance ecosystem as a whole we must consider how to minimize administrative burdens in order to support more effective compliance paradigms. Both regulators and organizations should focus on maximizing resources deployed towards effective privacy compliance and oversight; as noted above, too many resources are allocated to burdensome administrative procedures of registration and notification that provide very limited compliance or privacy benefits.

Finally, we would like to address the proposal for the development of universal principles. However, for such principles to be effective they must incorporate and bridge the philosophical, legal and cultural bases of privacy across geographies. It is unlikely that such principles will create one universally applicable regulation or legal framework, but rather foster the development of inter-regional exchanges of personal data; the desirable result being the enablement of increased data flows that meet legal and cultural needs across jurisdictions. We also note that the OECD Guidelines on the Protection of Privacy and Transborder Data Flows and the APEC Privacy Framework are good examples.

We look forward to working with the Commission, related Authorities and the broader stakeholder community in this important consultation and revision process. We would be happy to provide the Commission with further information or clarification of these comments to assist the consultation process.

The International Chamber of Commerce (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. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the last century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".
ICC has three main activities: rules-setting, dispute resolution and policy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.
ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice.
Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on vital technical and sectoral subjects. These include financial services, information technologies, telecommunications, marketing ethics, the environment, transportation, competition law and intellectual property, among others.
ICC enjoys a close working relationship with the United Nations and other intergovernmental organizations, including the World Trade Organization, the G20 and the G8.
ICC was founded in 1919. Today it groups hundreds of thousands of member companies and associations from over 120 countries. National committees work with their members to address the concerns of business in their countries and convey to their governments the business views formulated by ICC.

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 through its initiative, Business Action to Support the Information Society (BASIS http://www.iccwbo.org/basis).