AmCham EU's response to the Trusted Cloud Europe Survey

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled €2 trillion in 2013 and directly supports more than 4.3 million jobs in Europe.

* * *

CONSULTATION RESPONSE

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts 53, B-1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: Roger Coelho rco@amchameu.eu +32 (0)2 289 10 18

2 May 2014

AmCham welcomes the "Establishing a Trusted Cloud Europe" vision paper

AmCham EU welcomes the 'Establishing a Trusted Cloud Europe (TCE)' vision paper which was released on 21 March 2014. We do so because the document provides a positive policy vision for cloud in Europe and we are pleased with the explicit suggestion to work towards 'building of a Single Market for cloud computing'. The paper highlights the economic importance of the cloud to European competitiveness – up to 1 Trillion Euros of GDP contribution and 4 million jobs in 2020. It also highlights the potential for efficiencies, enhanced services for SMEs and the potential for new business models and services that could evolve.

Yet it also importantly recognises that these are 'potential' benefits that are predicated on having 'the right policy framework'. The promise of the continued or expanded 20% growth rate in the expansion and adoption of cloud is with: *'... the support of an efficient EU wide single market for cloud services based on best practices, a common understanding of regulatory requirements and the most effective way of meeting the needs of specific cloud use cases'.* This is the central theme of a TCE. It also importantly includes the *'... elimination of regulatory and market access barriers at both national and EU level'* as an essential step in the process.

Understanding the complexity of cloud computing

All of these elements are essential. The focus on use cases is very welcome because it highlights that the cloud does not create a unitary set of issues and is not subject to a one-size-fits all solution, as well as highlighting specific issues that may be unique to sectors, data types other regulatory obligations. In addition, they also demonstrate where commonalities of approach or treatment may exist, at least in part.

The use cases are also important examples that demonstrate how regulatory construction may serve as an unintended impediment to innovation, as well as the use and implementation of new business models. It is preferable for legislation to set out the objectives and to leave the stakeholders to decide what is the best way to achieve those objectives (please see AmCham EU Position Paper on Cloud Computing – 15 April 2013).

Addressing regulatory barriers

TCE's methodology is predicated on the development of instruments (code of conduct, SLA guidance, Safe Contracts etc. – each designed to meet EU compliance requirements) that can be voluntarily adopted to demonstrate compliance with EU legal requirements and norms. This process of adoption is supplemented by best practices, common standards and templates addressing risks, data types and use cases that would create a common framework.

Some concerns related to implementation

While the voluntary nature of this construct is welcome, this is where concerns related to implementation arise. Within TCE there is recognition that one size doesn't fit all, yet there is a failure to grasp the level of complexity of the cloud. Much of the common framework may well apply to public cloud where there is often less potential for negotiation, but is much less applicable to the more highly negotiated private cloud and may have complex applicability in a hybrid cloud. Indeed, 'cloud' as such is merely an efficient technological delivery method of computing power, whereas 'public', 'private' and 'hybrid' are various deployment models of that method. While the notion of a common framework sits well with the public deployment model, private and hybrid cloud offerings provide precisely the flexibility needed to address those customer needs that cannot be adequately served solely by public clouds operating on standard terms and/or in common frameworks.

Bolstering the uptake of the cloud as a delivery method in Europe should happen in an agnostic way: the objective of any common framework under TCE should be to preserve the diversity of services on offer, and to help customers make educated choices as to which particular deployment models, public, private or hybrid, are

best suited to their particular needs. However the framework should not, whether intentionally or inadvertently, drive customers to favour one model over another.

Similarly, differentiation in the use cases is not really made in a coherent fashion based on users/providers (B2B, B2b, b2b, B2B2b/c, B2C, b2c, c2c, and all of the possible 2G variations[1]) or the nature of services (IaaS, PaaS, SaaS – different use models have different implications related to data, its location or use). Application of a common framework that does not have the correct level of tailoring or nuance can lead to constraints on innovation and implementation that would clearly limit the potential of the EU to meet its desired goals of economic growth, job creation and enhanced efficiency. Furthermore governmental action to better define, clarify and harmonize requirements, like in the proposed one stop shop in the draft data protection Regulation and requests by entities already covered by other sectoral regulations to have those obligations recognized will go a long way towards creating a workable common framework[2].

It has also been our experience that voluntary programs can approach the status of soft law, if not actual compliance requirements, when they become part of government procurement regulations, and that transformation is also often adopted by private sector actors. An insufficiently nuanced common framework could unfortunately serve as a limitation, as opposed to facilitation, of cloud adoption in the EU. To avoid this, we encourage all stakeholders, including policy makers, cloud providers and public and private cloud users, to sustain an open and transparent dialogue on the precise needs the common framework is meant to serve, on the difficulties it is meant to overcome, and on the various solutions it should encourage. The collaborative identification and the pragmatic and flexible resolution of issues is in all stakeholders' shared interest.

Building trust

Lack of trust and understanding are also identified as major obstacles to cloud adoption in the paper. The lack of trust is noted to have heightened after the recent revelation of access to information by, and sharing of information among, global intelligence agencies. We recognize that trust is a legitimate issue at governmental, corporate and individual levels, but we would also caution that the trust issue has been exacerbated by a combination of misinformation and misunderstanding. Governments have a legitimate role to play in protecting the safety and security of their populations and this involves the use of appropriate intelligence practices. What is at issue is the question of what type and how much surveillance is appropriate and subject to what oversight, due process and redress. This is of necessity a conversation that can only be truly resolved at the intergovernmental level.

Many companies and individuals have voiced various corporate and personal positions on these issues, and the current societal dialog on the topic has been useful to inform decision-makers. However the actual decisions remain entirely in hands of governments. Business has been consistent in urging governments on all sides of this issue to engage in constructive dialog and to find common grounds for solutions (please see the AmCham EU Position Paper on Cloud Computing – 15 April 2013).

While businesses all share a priority in protecting the information, confidentiality and privacy of the information of their customers, they are also bound to comply with laws of the countries in which they operate. American companies operating in the EU must comply with EU laws, including those of privacy and lawful access requirements, just like EU companies operating in the US must comply with sectoral privacy laws and lawful access requirements. Business has no desire to compromise the privacy of its customers, nor does it wish to unknowingly be of any assistance to any criminal or terrorist activity. Only intergovernmental agreements can properly address these questions. In the interim, businesses do what they can to safeguard information, require

[1] Please note that small 'b' is used to denote SME

[2] We also take note of the work being undertaken between the APEC Data Privacy Subgroup and representatives of the Commission, EDPS and the Article 29 committee on interoperability between EU Binding Corporate Rules and APEC Cross Border Rules as a positive example of global policy interoperability which could also support broader common frameworks.

appropriate legal procedures be followed and provide the information they are allowed to concerning requests for disclosure.

In that sense AmCham EU was encouraged by a recent decision taken by the Article 29 Working Party showing that non-EU companies can also offer cloud services to European customers in compliance with EU data protection laws. Nevertheless, a simplified contractual framework for achieving adequate data protection for cloud services would be very helpful. With the current tools, the challenge for cloud service providers of putting a global privacy compliance framework together may be a roadblock for new entrants on the market for cloud computing even though they have a clear desire to offer their European customers an appropriate level of data protection that.

While we believe that enhancing the concept of trust is very important, we do, however, not believe that the principle of a "Trusted quality Cloud Europe mark/brand" is the best way to do it, as the disadvantages outweigh the advantages. It could for example be perceived as a trade barrier, causing other countries/regions to create genuine barriers using the need for such a mark as a pretext, thereby damaging European cloud providers.

Fitting Europe into a global digital economy

With that in mind, we very much appreciate the statement in TCE that:
'It is clear that the economic potential of European cloud services depends on the ability to avoid any semblance of a 'Fortress Europe' model where access to the European cloud market is de facto restricted to providers established in the EU. Non-European cloud providers should be able to access the European cloud market on equal terms and offer services that adhere to best practices...'

As was noted in our continued calls for intergovernmental dialog, the ECP similarly notes that resolution of issues related to surveillance and national security are beyond their remit. They propose useful suggestions on EU Member States entering into multilateral cooperation agreements, but again, those are within the sole responsibility of governments.

The reality is, however, that if these issues are not addressed in a constructive fashion, the benefits and opportunities of the cloud will never be fully realised. Furthermore, the possibility of retreating into a 'Fortress Europe' will become an unfortunate reality in which efficiencies of scale and scope could be lost, fewer services may be available to European citizens and at potentially higher cost, and global information and trade flows would be saddled with needless burdens and unintended consequences. This more limited Transatlantic if not global interchange may well result in diminished innovation as exposure to cutting edge technologies or business models may be unintentionally constrained. We continue to call for constructive and productive dialog between all governments concerned in the interest of enhanced opportunity, economic growth and societal benefit.

In considering the TCE at a detailed level and possible improvements in its messaging, more attention also needs to be paid to the use rather than simply the provision of cloud services. The greatest economic and societal leverage of the cloud comes from running applications and business models - not providing the three basic services of the cloud. While it is legitimate for both objectives to be pursued, the TCE seems more focused on provision of, rather than use or leverage of cloud services. This focus may leave the largest potential benefits unrealized. Furthermore inadvertent limits on services as highlighted in the preceding paragraphs may likewise needlessly limit the potential economic and societal benefits of cloud from being realised.