OpenForum Europe Response to "The Future of Cloud Computing, Opportunities for European Cloud Computing Beyond 2010"
15.02.2010

Response by: OFE Limited
Register No: 2702114689-05
Contact address: BISCHOFFSHEIM BUSINESS CENTER
Boulevard Bischoffsheim 36,
1000 Bruxelles

1. Summary

OpenForum Europe (OFE) very much welcomes the timely publication of this report. OFE sees it as a valuable contribution to both the understanding of the opportunity and the new challenges that it raises. It comes at a time when OFE is about to publish its own Introductory White Paper on Cloud Computing, and it is good to see a high synergy in the core thinking of both documents. As an organisation whose prime mission is in support of a competitive, open ICT market it will be no surprise that in this response we have focussed on those issues in which we can be expected to have strongest interest and knowledge, in particular "openness".

Cloud Computing can not be dismissed as yet another market hype. It is already rapidly progressing and is likely to present the next paradigm shift in the ICT market, creating discontinuity to users, suppliers and legislators. Proponents of the Cloud will point to many potential benefits including cost efficiency, accessibility, pace of innovation potential, improved business collaboration,reliability, and sustainability.The Cloud offers specific benefit to SMEs, which will be particularly important for European business, and their specific needs will require particular focus for the Commission.

A macroeconomic study on the potential economic benefits of cloud computing in European Union countries attempts to estimate the impact of lowering the fixed ICT cost of entry into a market for companies, especially for SMEs.[1] The study forecasts, over the next five years, a 0.1-0.3% increase in GDP, the creation of 84,000-430,000 new small and medium size businesses, and 300,000-1.5 million additional jobs (which translates into a drop of the unemployment rate by 0.3-0.6%).
The conservative assumptions such as a reduction of total enterprise costs between only 1% and 5% make it likely that the economic impact of fast adoption may be considerably higher. Moreover, the model does not take into account other factors such as the potential increase in productivity through better collaboration in the cloud.

[1] See Prof. Federico Etro, "The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe", see http://www.intertic.org/Policy%20Papers/RBE.pdf. See also a Meryll Lynch research note "The Cloud Wars: $100+ billion at stake" (07 May 2008) which estimates cost advantages of 3-5x for business apps, and 5-10x or better for personal productivity apps.

But realisation of these benefits will not be without barriers and challenges which will impact European strategies, policies and potentially legislation. These include Open Standards, data interoperability, data portability, security, privacy, open access, and accessibility.

Central to success will be the ability to maintain an open approach, not just to the core infrastructure but to all technological aspects of interoperability, portability and ownership in a way we see the internet is today. Commercial pressure to seek to re-introduce proprietary lock-in will be inevitable as existing ICT suppliers seek either to resist the new competitive models or wish to exploit the potential in a way detrimental to European policy and consumer interest.

2. Comments on the Report

Definition

With the technologies concerned still in their infancy, it is not surprising that there is still no single widely shared definition for Cloud Computing. While the report adds another definition (p.8), we would like to point to the definition used by the US Federal Government and its NIST agency which define Cloud Computing as follows:

> "*Cloud-computing is a convenient, on-demand model for network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*" [2]

In many ways, it can be helpful to think of Cloud Computing as a **transition**. The scale of that transition is dependent on a number of factors, all of which combine for the complete shift to take place, but each element is valuable in its own right:

- Firstly, the type of activity has sufficient volumes to support service provision. As competition increases it is likely that the required number of users will decrease over time.
- Second, a multi-tenant application or shared infrastructure approach, is also present.
- Third, "virtualisation" technologies (ie. to enable data to be packaged up ready for transfer and reuse in the cloud) are adopted and will be further improved and standardised.
- Fourth, the web-based model - with cloud applications being accessed primarily through web browsers — supported by ever increasing ubiquitous networking. This trend relies on innovation in browser software and standards to deliver a faster, more stable and richer user experience.
- And finally, human attitudes - whether for consumers, government or enterprise - need to understand and embrace the implications of the cloud model for their organisation and adapt their process, IT policies, procurement behaviour and in some cases legal frameworks accordingly.

Recommendations

OFE wishes to comment in particular on the following Recommendations made in the paper:

Recommendation 2: The EC together with Member States should set up the right regulatory framework to facilitate the uptake of Cloud computing.

The Cloud will challenge many current existing proprietary business models and definitions associated with openness, and indeed the current openness of the internet itself. This will involve those aspects introduced above such as data portability, application transparency, security and privacy. The recommendation suggests that the specific issues are Economic, Legalistic and Green IT. In the same way as Green IT has been highlighted we would suggest that "Openness" should be added as specific focus.

Additional Recommendations 3 and 4

[2] See p 158 at http://www.whitehouse.gov/omb/budget/fy2010/assets/crosscutting.pdf
as well as NIST at http://csrc.nist.gov/groups/SNS/cloud-computing/

Together these recommendations rightly give considerable recognition of the potential importance of both open standards and open source. We endorse the contribution that Open Source can be expected to make. We already observe high discussion within the community on a range of issues ranging from applicability of licensing options through to delivery of services based solutions. We would strongly recommend early engagement in these discussions.

Openness and Interoperability

Bearing in mind the strong recommendations in support of open standards and open source we are therefore surprised that the issue of openness of solution is not given more attention in the report.

We would also suggest that interoperability between different clouds should be added as a research challenge to the document. This impinges not just on the clouds themselves but the parallel maintenance of an open internet.

3. Openness as the Basis

Openness is more than just the adoption of Open Standards (but see this discussed below). Lock-in can occur from many different quarters, technological and commercial. So the issue of openness will occur not only on the accessibility and interoperability between clouds, but also the ease by which a user can move data, and substitute services.

Each of the delivery models normally associated with Cloud Computing will impose different requirements on the need for Open Standards.

In the case of 'Cloud Software as a Service' many of the requirements will be a repeat of those already being discussed, notably standards for interoperability. Notably Open Document Exchange Formats (both for editable and non-editable documents) will remain paramount. In the context of the Cloud, however, data formats are now joined by data portability as an issue.

For 'Cloud Infrastructure as a Service' and 'Cloud Platform as a Service' the openness of the APIs used within the framework become even more critical.

Across all three deployment models, which will remain fundamental in Cloud Computing, is the additional key aspect of an 'open internet' in respect to access. Ensuring a fair, non-discriminatory, transparent and competitive playing field (the European Commission Communication on Future Networks & the Internet in 2008 used the term “net neutrality”), is the principle that end-users can reach the Internet applications, content, and services they desire on a level playing field, without anti-competitive discrimination on commercial grounds, or restrictions. The Communication rightly stated that “traffic management could be used for anti-competitive practices such as unfairly prioritising some traffic or slowing it down and, in extreme cases, blocking it.” The conclusion of the Council of Ministers on the Commission's communication recognised "that open and non discriminatory access to the Internet should be promoted in order to ensure effective competition and an innovation-friendly environment."

We agree that while Internet traffic can be duly managed to guarantee quality of service at busy times, there is no place for anti-competitive discrimination that prioritises some content over other as a function of commercial ownership, agreements, or interests. There should be a principle requiring non-discrimination between comparable services on the same underlying infrastructure (i.e. within the same class of use from the perspective of the end-user; for instance, IPTV services will certainly compete with video-streaming platforms so they should be considered to be comparable services). This does not prejudice the right to undertake reasonable network management if and when necessary to address congestion at peak times (for instance by prioritising latency-sensitive applications to ensure quality of service), or improve specific services with investments in networks and infrastructure enhancements.

4. Barriers and Challenges for the Uptake of Cloud Computing

Cloud Computing faces a number of barriers to adoption and throws up a number of important challenges, in terms of strategy, policies and potentially legislation, which may need to be addressed if the model is to fulfil its potential to drive economic and social value, not just in Europe but across the world. OFE believes of these should form the basis of the studies which support *Recommendation 2* of the Report.

Open Standards, data and application interoperability. Open Standards ensure that neither prior permission nor royalties are required to implement them and that companies can freely create products which interoperate with others across the Internet. It will be crucial for realising the promises of Cloud Computing that data and applications be interoperable and use Open Standards where already available. While the Internet moves very quickly and the Cloud is in its infancy, standards organisations do not move at this pace, so there is inevitably a time lag before standards emerge from an open, collaborative process. At a minimum, fully and completely disclosed, and effectively implementable Application Program Interfaces (APIs) are an essential element for interoperability that providers need to support. Interoperability among the various clouds will be a crucial enabler for innovative applications. As stated in it's Communication on the Future of the Internet of November 2008, the European Commission recognises that "the win-win of open interfaces and Open Standards is that the market can grow for all."

It also correctly acknowledges the risk that "dominant players may try to use proprietary standards to lock consumers into their products or to extract very high royalties from market players". The move to a distributed Cloud Computing model based around the open protocols and standards that have driven the development of the Internet is a challenge to other more proprietary-based computing models based around the client-server model. Policy makers, will need to ensure that as Cloud Computing develops, dominant companies in client desktop operating systems and the browser markets do not leverage their distribution power by spreading Internet technologies based on closed standards which create new dependencies on the dominant platform, as this could ultimately lead to lock-in and limited consumer choice. A typical detrimental behaviour witnessed time after time in the PC environment would be to offer initial support across platforms for a proprietary technology based on closed standards, just to withdraw that support once the technology has gained widespread acceptance, thereby locking consumers into the existing dominant platforms.

The community has not been slow to suggest standardisation as a route forward and indeed at the last count some thirteen standards setting initiatives have already emerged, each with a different focus and degree of representativity. Such a plethora is both positive, due to the recognition of the potential issue at this stage in the development of the market, and daunting because of potential conflict, confusion and division.

Data and application portability to address user lock-in and ensure user trust. Ensuring that data and applications can move between providers or back in-house at will, is a concrete implementation of openness that can and should be implemented by every single cloud provider and which does not depend on the agreement of open cloud standards. An example is an initiative by a team of Google engineers called the "Data Liberation Front". This team builds data export functionality into Google products.[5] There is still much work to be done for cloud providers to ensure data portability to avoid lock-in of users in the long run, so that the owners of data and/ or applications can easily, and at no extra cost, export their data into common formats and communicate via open interfaces.

Users expect to be able to own their data in the cloud just like they do with data on their own computers. Therefore, user should be able to easily export their data from a company's services if they choose to do so. Enabling individuals to take their data stored in any given service of a company and move it to a different provider or system does not only prevent lock-in, but is also a means to revoke trust that had been granted earlier. Privacy practices can evolve over the years, as can user preferences over products or privacy of an individual user. Giving users ownership of their own personal data and providing them with the possibility for revoking prior decisions is key to promote trust into the system and the future success of this model and will undoubtedly help stimulate interest in and demand for cloud services.

Security. Cloud Computing is a new paradigm, where users (or organisations) cede control over the technology infrastructure that supports their data to a third party. Users' data and the software and hardware that process it are no longer located on the user's premises or within the organisation's firewall. This psychological shift implied by the lack of immediate control can lead to a feeling of insecurity - similar to the common perception by an individual that flying is more risky than driving, although the opposite is true. This perceived reduction in security can act as a barrier to uptake of the cloud.

Cloud Computing is a paradigm shift, similar to taking your jewellery out of your sock drawer and placing it in the bank. The bank has the economies of scale. It has guards, robust safes, video surveillance — much more than any security investment you can deploy yourself. The same is true with data. Cloud providers are equipped to protect millions of users' data every day. Costumers get to enjoy these economies of scale at minimal expense.

While no computing model can ever offer 100% security – as many years of experience with desktop computing models and smaller incidents with cloud services have shown – there are reasons to expect that cloud services prove to be more secure, in particular in comparison to local infrastructure run by those users and organisations that lack the expertise and/or resources to run professional software and network security policies – the very large majority of users. First, by not storing much data on local devices, the cloud mitigates one of the most common security risks for users, that of data loss at the end point when e.g. a laptop is stolen, a USB stick is lost or an attachment is accidentally emailed outside the company. Second, the cloud can be a driver to security due to its simpler architecture, the professional maintenance of the infrastructure, and the ability to effectively and frequently role out security/ software updates without the need for any action by the user. Most organizations today take 30-60 days or even several months to install security patches on their systems which is a major concern in its own right. This means that traditional IT systems and applications are open to known security vulnerabilities for a very long time. By contrast, cloud providers run a very homogeneous computing environment, so when it is time to patch this can be done in a rapid and uniform manner to all systems at once.

Whichever computing model is used, the security of the IT infrastructure is only as strong as its weakest link, and joined up thinking across public and private sector is needed, in particular also with regard to the governmental sphere. That said, providers of all computing platforms will need to make a compelling case for security and differentiate themselves on their security credentials, with a dynamic marketplace reflecting user perceptions. Any system can be affected by some security issues. The real question is what people, process, and technologies are in place to minimize the impact of these incidents, and how quickly one can respond if anything goes wrong.

Another issue is the cloud's ability to let cloud customers - in particular organisations using the cloud - integrate their own security policies. Customers expect similar insights that they have into their data centers.

Privacy - the emergence of the Internet has turned the spotlight on the appropriateness of existing privacy legislation for today's society. Important principles established in the 1995 EU Data protection Directive continue to be fit for purpose, however there are concerns with the complex implementations that this has given rise to, and the complex and scattered governance system which underpins the enforcement of privacy legislation. It's important to ask how our privacy laws and regimes can deal with this new computing paradigm.

First, the 1995 Data Protection Directive bases regulation in part on the location of data. However, it is actually very difficult to answer the question where cloud data is stored. Data in the cloud exists within the physical infrastructure of the Internet on the servers of the companies offering these services, as well as on users' own machines. Users of cloud services expect their provider not to lose their data and to respond to their queries quickly. Data centres therefore usually replicate users' data in more than one place, optimize the location to enhance the speed of a service, (such as serving European users from a European data centre), and optimize computing power, automatically shifting work from one location to another, depending on how busy the machines are (e.g. when more capacity is needed in North-America and capacity is available in Europe during night, European data centers may serve North American users). Therefore, instead of a location-based model, the fundamental question, to determine how a user's data is being protected, is who

holds the data, and what are a provider's privacy policies. Legal provisions should rather apply to the data controller regardless of the physical storage of the data. In addition, global minimum standards for data protection become increasingly necessary in a world where data flows around the planet at the click of a mouse, but three out of four countries do not have any privacy laws in place whatsoever.

Second, EU laws impose restrictions on the transfer of personal data outside the EU to any jurisdiction where there is not "adequate" data protection. In the past, "transfer" was defined as the physical shipment of data. However, nowadays almost any activity on the Internet involves a transfer of data outside of the EU. Sending a document to a person in Toronto, for example, may technically be considered a transfer of material outside of the EU. In today's era of connectivity, strict and literal application of these laws written in the pre-Internet era would cause more than just a headache for companies and regulators: it would cause the Internet to shut down. In contrast to the EU's state-to-state approach, Canada has, through the PIPEDA Act, chosen an organization-to-organization approach where organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement.

Third, to ensure users' trust policy makers should ensure that the privacy laws apply standards of protection from unauthorized access by governments to data stored in the Cloud that are equally high than the standards applying to data stored on devices located at a user's home.

Inter-Cloud Communication as a Research & Development challenge. With Cloud Computing still at its infancy stage, we today face the challenge that much needs to be done to develop better communications between clouds developed by different vendors. The protocol and code to express the idea of “another cloud” needs to be developed. Tim Berners-Lee, the father of the Web, promoted the idea of "data linking" and to develop vocabulary in which actions on data can be expressed. This could be the beginning of an inter-Cloud Computing language which would effectively constitute a new layer in the Internet architecture.

Open Broadband Access - Cloud Computing could only emerge with the increasing deployment of high bandwidth Internet connections, which reduce response times and make the cloud experience comparable to the desktop experience. To enable more people to benefit from Cloud Computing, governments can help with policies that ensure all users can be connected to the Internet all the time. The specific measures envisaged may be different in each market, however ensuring competitive broadband access markets, fair and non-discriminatory access for Internet services and a liberalised wireless spectrum are key ingredients in the policy mix. Once services are deployed, regulators must rigorously ensure that traffic management activities of network operators do not discriminate between competing applications, services and content.

Organisational Challenges – incorporating Cloud Computing within existing IT infrastructures will necessitate organisational changes which will require careful management, particularly in a public sector context: relationships with existing staff, suppliers and systems integrators may be affected by moves to outsource IT functions along the cloud model, and may create resistance to change away from legacy operations. Internally, too, the challenges are not to be underestimated. IT departments of larger organisations are adept at managing change and may deploy a mix of processes or applications depending on the maturity of the process or application: innovative, customised applications that seek new ways to address emerging problems, as well as standardised and repeatable services that aim to deal with volumes of predictable data and reduce deviation from set parameters. Different methods are needed to control these different procedures, but the introduction of Cloud Computing to structure and decentralise innovation will add to these management challenges.

Transition to Cloud Computing – adopting Cloud Computing is not as simple as transferring data into online applications. Indeed, there are a range of legal, financial, contractual factors to consider and manage before an organisation may be ready to make the transition to the Cloud. At present no comprehensive models exist to validate an organisation's readiness to make such a move, and advice on actions to be taken. Such a model would need to include considerations such as data portability, but also licensing conditions for software, terms of service, data ownership, and end-user license agreements. The rise of Cloud Computing is likely to increase IT users' appreciation of the value of interoperability and the ability to control and move one's own data. Such a model should help users understand the impediments to change, and the benefits of doing so.

Enterprise 2.0 and Government 2.0. With today's unparalleled innovation speed on the web, the consumer market routinely gets the greatest innovations first, no matter which web 2.0 application one considers. These technologies only migrate to the workplace once they have matured with consumers. For governments, the move away from an all desktop to corporate cloud may be slower still. Public procurement processes may need to be adapted, since they may be poorly-suited to leasing software as a service rather than purchasing software as a good. Or up-front costs to be recouped in outyear savings may prove necessary, along with pilot programmes to demonstrate capabilities, including appropriate security and privacy protection.6 Clear leadership will be needed to handle this disruption in a public sector context.

Accessibility- industry and policymakers have worked hand in hand for years to try and overcome the "digital divide" whereby some users find it more difficult to participate in the information society. The same commitment to provide access for all users should apply in the work of Cloud Computing, via the adoption of available standards for web accessibility, by ensuring accessibility by design of user devices, and by incorporating adaptive technologies wherever possible. Furthermore, Internet technologies can increasingly help improve access to information resources across cultural and language divides. Emerging automatic translation tools that "live and learn in the cloud" can help ensure that the bulk of Internet content – created in just a few wide-spread languages – becomes accessible to new communities of users.

Preservation – when faced with immediate access to huge volumes of data on a daily basis, it is tempting to forget the importance of longer term preservation of digital content. However ensuring long-term archiving and availability of digital content is a major legal, social, commercial and cultural challenge. Appropriate mechanisms and Open Standards need to be in place and adhered to, to ensure that our digital lives are not just available now, but accessible across time.

5. Conclusions

OFE is very pleased to welcome this draft report adding considerable value in the ongoing discussions on the importance and impact of Cloud Computing in Europe and in support both of the Digital Agenda and of EU2020. OFE does, however, suggest increased and specific focus is given to all the interoperability and access issues essential if the Cloud is to meet its full opportunity. The Commission is well placed to take a leadership position, while involving stakeholders, to encourage R&D as well as foster a regulatory framework that facilitates the uptake of the cloud.. For its part OFE and its members and partners who together contribute a major part of such stakeholders representing the open community would welcome to continue to be involved in this endeavour.

Notes

OpenForum Europe (OFE) is a not-for-profit member organisation based in both Brussels and the UK, established to support an 'open' and competitive IT market in Europe. OFE is supported by some of the most influencial ICT companies including Deloitte, Google, IBM, Oracle, Red Hat and SUN but also particularly works in strong partnership with a long list of both national and European partners.

OpenForum Europe acknowledges all the input received from its members and partners in the compilation of this document. However, OpenForum Europe does not seek to represent any specific community nor present their opinions as being unanimously supported by their full membership. References given are fully attributed and every effort made to ensure they have been taken in true context.

www.openforumeurope.org