International Chamber of Commerce
The world business organization

Policy statement

Prepared by the ICC Commission on
the Digital Economy

Business views on regulatory aspects of cloud computing

Contents:

Highlights

- Cloud computing represents a continuing evolution of technology that has increased in scope, bundling and geographic spread of services offered.
- Building consumer trust and confidence in cloud is key.
- Risks faced by businesses and consumers when dealing with cloud-based services are not new.
- Governments should be encouraged to use the regulatory powers they already possess in order to improve trust and understanding in the cloud services market.

Document No. 373/509 – (29 February 2012)

Introduction

Although the commercial implications of cloud for small and medium-sized enterprises (SMEs) and consumers may be revolutionary, it does not follow that there needs to be revolution in government's regulation of cloud services. While many issues related to cloud services may arise, most are either well within our experience curve or still evolving and not ripe for detailed guidance. Overly prescriptive measures or the anointment of "a" best practice where many practices may be needed can serve to limit the potential of emerging models and constrain innovation related to models not yet developed. Regulators and governments already have wide-ranging powers in respect of cloud-based services, particularly in the consumer arena

Building consumer trust and confidence in cloud is key. ICC believes that governments should be encouraged to use the regulatory powers they already possess in order to improve trust and understanding in the cloud services market. In the meantime, information is needed to help users make more informed choices among service offerings, terms and practices.

The reason that no specific new regulatory approaches are needed is that cloud computing represents a continuing evolution of technology. Most aspects of cloud computing have been in use in the business-to-business (B2B) context for years. In this context, cloud represents an evolution of technology that has increased the scope, bundling and geographic spread of services offered. Many of the 'regulatory' issues can, as now, be dealt with through proper contractual obligations. Practices, contract terms and provisions related to cloud services are continuing to develop with the evolving technologies and emerging business models.

In the case of large enterprises there is greater expertise and experience with these issues and related ones as well as greater likelihood of equality in bargaining positions. Furthermore, enterprise- cloud deployments often include customization or other unique services that need to be reflected in individualized contract terms.

For SMEs and consumers, while cloud services continue to represent technological *evolution*, they have the potential of creating more *revolutionary* business offerings in terms of new services and delivery mechanisms. But consumers and SMEs are initially less likely to have the knowledge or experience required to understand the possible legal and contract issues that may be relevant to cloud services. Finally, consumers and SMEs may have less bargaining power and will likely be relying on established service offerings where service variations are possible through in-built configuration options rather than customization to a single enterprise's needs.

It should be noted that established service offerings may provide substantial customization offerings for the end user; but these are choices among defined options rather that options developed or customized for the particular. Similarly, applications of mass deployment cannot accommodate customized terms, though there may again be options across the offering of terms and conditions (higher security, service levels or guarantees for increased costs). In many instances, customization and configuration menus available to cloud application users without deviating from standard vendors agreements are strongly influenced by end user and developer community debate and interaction with vendor staff using the Internet; in many cases such user-driven development of standard options lead to results comparable to, and often in the end drastically reducing the need for, customer-specific changes. SMEs and consumers can also participate in one of the more current aspects of cloud computing – enabling consumers and SMEs to provide business and social-based services facilitated by cloud technology.

SMEs and consumers differ slightly in two main respects. When resorting to cloud services, SMEs may require more specialization in the offerings they use which may mean that they are more likely to purchase offerings from smaller, more specialized or niche cloud providers that focus on their sector or vocation. These smaller providers, while having expertise in their services, may be relatively new to the complexity of cloud practices and contracts. Consumers, on the contrary, may be more likely to adopt highly standardized offerings. The second major difference is that 'consumer developers' of more social-oriented cloud services may do so on a voluntary, non-commercial basis, which may have significantly different legal implications and expectations than services that require payment.

Although the commercial implications of cloud for SMEs and consumers maybe revolutionary, it does not follow that there needs to be revolution in government's regulation of cloud services contracts. While many issues are and may arise related to cloud services, many are either

well within our experience curve or still evolving and not ripe for detailed guidance. Overly prescriptive measures or the anointment of "a" best practice where many practices may be needed can serve to limit the potential of emerging models and constrain innovation related to models not yet developed. Regulators and governments already have wide-ranging powers in respect of cloud-based services, particularly in the consumer arena. **ICC believes that governments should be encouraged to use the regulatory powers they possess, in order to improve trust and understanding in the cloud services market. In the meantime, information is needed to help users make more informed choices among service offerings, terms and practices.**

The desire or concrete plans announced by some governments to develop, operate or commission 'national clouds' is related to the issue of regulation. While it is understandable that governments want to take advantage of cloud benefits as a measure to make public administration more effective, it would be counterproductive if public sector clouds are positioned to compete with private sector initiatives.

This policy statement sets out international business views on regulatory issues in relation to cloud computing as a contribution to the on-going public policy debate on cloud as an important trend in Information and Communication Technology (ICT).

What is 'cloud'?

The definition of 'cloud computing' is daunting as 'cloud computing' means different things to different people. Some concepts of cloud can be seen as an update of concepts that reminds one of timeshared operations on mainframes. Other aspects of cloud are related to 'software as a service' or 'application service provider' business models.

Cloud computing is thus a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the 'cloud' that supports them.

The concept generally incorporates combinations of the following:

- infrastructure as a service (IaaS)
- platform as a service (PaaS)
- software as a service (SaaS)

Cloud computing services often provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers.
While much, if not all, of the technology related to cloud is familiar, the scope and type of use is new. Previous cloud-type applications usually required people to be in corporate or university settings to gain access to these benefits. Today's cloud applications can be accessed not only from individual personal computers, but more and more from mobile devices as well. Today's cloud represents democratization in terms of access to and use of cloud services. Some types of cloud also represent opportunities for individual developers to tap into large potential user pools. Thus the cloud is both old – in the sense of the fundamental nature of the services on offer – and new – in the sense of which parts of the market now have access to these services.

There remains no perfect definition of cloud that is applicable in all circumstances or shared by all communities, but many have recognized the National Institute of Standards and Technology's (NIST) definition as a positive step forward that represents many aspects of common understanding. The Computer Security Division of the NIST defines 'cloud computing' as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics:

***On-demand self-service*:** A user can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

***Broad network access**:* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants).

***Resource pooling**:* The provider's computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. To meet the user's short term needs, the allocated resources may see themselves expanded automatically to quickly scale out, and rapidly released to quickly scale in. To the user, the capabilities available for provisioning thus often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service: cloud systems automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Benefits of cloud

The benefits of cloud are wide-ranging and reach different sectors of the market in different ways. They include:

- increased productivity by allowing businesses to focus on their core competencies and customer offerings rather than IT infrastructure and maintenance,
- economies of scale through use of data centres that are more energy efficient and environmentally sustainable,
- reduced operating and capital cost,
- greater speed to market by reducing solution deployment time by leveraging cloud infrastructure,
- dynamic increased capacity and the ability to cater to business peaks without investing in infrastructure,
- transformation of organizations' fixed cost into variable cost,
- up-to-date software, professionally managed,
- consumer access to all applications,
- improved security through centralisation where cloud vendor is reliable and less expertise existed in company/individual,
- new business opportunities and new markets by offering high computing power at lower cost,
- faster and cheaper innovation by providing an existing platform for developers to build on,
- leverage on cloud computing for reliable and scalable backup and recovery facilities for Disaster Recovery (DR), and
- low barrier to entry, which can foster innovation and entrepreneurship.

Risks of cloud

In some ways, the discussion of 'risks' within the cloud space does not raise new issues as they are risks that are familiar to larger organizations who have contracted for Internet-based outsourced services similar to cloud-type offerings. Those risks have been successfully addressed in an outsourcing context. The first approach by policy-makers should therefore be to build on that experience.

(a) Security and Privacy of cloud-based data

Cloud computing by definition involves accessing services over the Internet. Already today many services include global information flows facilitated by the Internet, whether obvious to the end user or not. But cloud will broaden and accelerate the movement of data. Therefore, keeping data secure is of critical importance for all users - governments, organizations and individuals. Concerns about privacy and security are often used as key justifications for not migrating to cloud-based IT services. The migration of data over the Internet and into the cloud does not make data any more vulnerable than it was when secured internally; however, this movement and remote storage does make data in the cloud a target from attack that differs from what organizations and individuals are typically familiar with, and by virtue of its scale a more attractive target to attack.

Policymakers, and others involved in cloud need to demonstrate that they take these concerns seriously – otherwise cloud services will not be taken up. The reputational risk to cloud vendors that might result from data loss or compromise makes them strongly incentivised, in addition to their technical expertise, to address these risks well. But the risks should not be exaggerated.

For example, in some ways cloud computing services may offer increased data security, privacy, and reliability. With the PC-based computing model; when a PC is lost, stolen, destroyed, or compromised, data can be permanently lost or, worse, extracted to reveal personal or proprietary information. In addition, many organizations, especially consumers and SMEs, do not have the technical staff to assure that systems are patched, tested and appropriately backed up. Furthermore, for many computer users with limited technical support and capacity, security is accomplished by locks and doors and imperfect passwords. The laptop or server under a desk is no match for a level 4-data centre. The cloud model provides enhanced reliability because data is backed-up over the network at multiple locations hosted by the cloud computing service provider eliminating the single point of failure concern. This added reliability is essential for individual users and organizations that hold sensitive and personal data, such as health care providers, financial institutions, and government agencies.

(b) Access and broadband deployment

Cloud computing allows users ubiquitous access to computing power, storage, and applications. This universal access means that users are no longer tied to a specific device. Since applications and data are stored in the cloud, any device that can connect to the Internet can also access data stored in the cloud from any location. Also, universal access means that multiple users can access the same applications simultaneously regardless of their location, which can increase productivity, collaboration, and information sharing.

Because applications and data are hosted in the cloud and not stored locally, when the network fails users cannot access the cloud. Potential users may view migrating to the cloud as a risky proposition if broadband networks are non-existent or unreliable. Therefore, when users are considering migrating mission critical data or applications, they must always consider the potential for a failure of communications, potentially due to external catastrophic events. Strategies for cloud migration of critical resources should consider issues of disaster-preparedness and recovery.

(c) Contracting

Contracts with major cloud computing providers are similar in scope and negotiability to contracts that are found in other areas of the information technology ecosystem. There are two broad categories:

- *Common word processing, mail services.* Contracts for office-based services of cloud-based services (e.g. email, word processing, spread sheets, etc) are quite similar, conceptually, to licensing contracts found in the non-cloud environment (*e.g.,* "shrink wrap" agreements for software bought and installed on a personal computer) or for the use of services in the Internet (*e.g.,* "web wrap" and "click through" agreements found on websites). Because of the scale of the services provided, there is often very little opportunity to negotiate agreements individually. That should not be confused with a lack of choice. SMEs have "menu options" they can choose from in the course of selecting their contract (as to security standards for example, or hours of support, or nature of data transfer activities on exit), but these will typically be in the form of largely standardised modular offerings, as in the software licensing industry today. **SMEs should, therefore, expect about the same (limited) level of negotiation ability for service agreements for office-based cloud products as they do in these other contexts.**

- *Preservation of Data.* In the traditional office context, companies and users rely on the integrity of their hard drives and related back-up systems. These systems, like other contexts, are governed by warranties that may guarantee the replacement of the hardware, but which do nothing to guarantee the integrity of the data. This is one area where cloud computing offers significant contract benefits. While contracts for data storage are often not negotiable (any more than warranties are in the computing ecosystem), there is a highly competitive market for data preservation. **Companies should look for contracts that allow for: data portability and export and that provide redundancy and secure data in diversified ways to facilitate data recovery.**

Cloud computing services depend heavily on fast and stable connectivity to the Internet. Purchasers of cloud services can often buy various tiers of service from Internet Service Providers (ISPs) that assure different levels of speed, latency, and connectivity. **Cloud providers often provide guidance to their customers as to the minimum technical expectations required in this regard, and businesses should be sure to contract with their ISP for the appropriate level of service.**

While large providers can do little to customize mass offerings beyond providing menu-driven choices, **users should consider that smaller providers and providers seeking to serve niche markets may provide services more tailored to specific needs.** Issues related to selecting these providers will revolve around evaluating the services offered and the reputation/capabilities of the new entrants. Reputation and other third party evaluation and certification services may emerge to help users of these services make more informed decisions.

Regulatory response

Just as cloud computing poses no new risks to business, it follows that the regulatory challenges of cloud computing are no different from the challenges faced by businesses in outsourcing operations over the last twenty years. The costs and scale of cloud computing may have brought the regulatory issues to new types of customers (consumers and SMEs who perhaps could not previously engage economically in the outsourcing market place), but the challenges for regulators are both well-known and well worn.

It follows that governments should be reluctant to regulate cloud computing afresh; they should however continue to monitor the cloud services market regarding privacy and security issues. The main near-term focus should be on how to properly apply existing regulation to cloud environments which may have more jurisdictional complexity.

Regulation of the cloud today

Although regulation and perceived regulatory risks in relation to cloud services cover many areas of law and regulation, there are in our view four broad categories of particular importance to providers and consumers of cloud services:

***Data privacy*:** these are regulatory obligations derived from the personal nature of the data a customer places in the cloud. These types of regulations typically impose obligations, usually on owners or controllers of data, about keeping information secure, notifying individuals when their information is lost and requiring oversight of contractors who might get access to this information. Although the EU Directive 95/46/EC is a well-known example, this is not just an EU issue. For example, important work has been done in APEC on implementing a privacy framework based on accountability. Concepts of accountability are especially important in cloud contexts as they more easily enable obligations to flow with the data. As opposed to requirements based solely on the laws of the jurisdiction where information is processed, accountability mechanisms, like the APEC example, embody negotiated common principles that, for the jurisdictions involved, adequately reflect the key tenets and enforceability of their own national or regional rules. The potential merits of accountability mechanisms today have great currency, and in no small part, trace origins to the principles of the 1980 OECD Privacy Guidelines and PIPEDA, the Canadian Privacy Law.[1]

Market practice, co-ordinated action by organizations such as ICC and regulator guidance have created possible solutions to the challenges posed to handling personal data in an outsourced environment, which can function just as well in a cloud environment. Where those regulations, and the existing solutions to them, have been ignored in a cloud environment, regulators have already been quick to take action.

***Confidentiality and secrecy obligations*:** these are regulatory or contractual obligations derived from relationships – such as that between a banker, broker, auditor or lawyer with his client or a doctor with his patient. They prevent disclosure of the secrets or confidential information entrusted to a "secret bearer". Although perhaps not as developed as in relation to data privacy, professional practice guidelines regulatory guidance and market practice has evolved in order to deliver effective outsourced service models that respect these obligations appropriately, either by (i) obtaining appropriate consents from clients or patients; (ii) ensuring that access by suppliers to data is prevented such that no disclosure of the secret or confidential information takes place; or (iii) allowing access by suppliers to data in a controlled way, with measures in place to preserve its confidential nature. As with data privacy regimes, these rules tend to impose obligations on the owner or custodian of the client/patient relationship rather than their suppliers.

Litigation and investigatory access: as described earlier, the flexibility afforded to businesses by cloud solutions may result in data of a customer moving across borders, perhaps even residing in multiple jurisdictions at the same time. That movement of data across borders exposes data to different regimes for access both in civil litigation and regulator backed investigations. Subsequent disclosure of that information, by a service provider either compelled to comply or voluntarily complying with a court or regulator request, may put customers in breach of rules prohibiting co-operation with foreign litigation or investigatory action. Those risks are not, however, exclusive to cloud computing or even outsourcing as a whole – they are for most organizations inherent in doing business, whether purchasing or sales, internationally.

***Specific sectoral rules on outsourcing**:* these are rules focussed on the controls necessary to manage the risks of any outsourcing, and are most prevalent in the financial services sector. For example, the Markets and Financial Instruments Directive requires any European financial services firm that outsources material functions to the cloud to have a range of contractual and practical protections in place, such as audit rights for customers and regulators and service continuity on termination. Although those obligations carry burdens and costs for both suppliers and customers, they have been in place for many years and all significant participants in the outsourcing markets are able to adapt to their requirements. As with privacy compliance, attempts to avoid these rules in a cloud context have been met by swift regulatory action.

---

[1] *ICC Data Protection Principle of Accountability Discussion Paper*, 23 January 2012, document no. 373/508, accessible at: http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/ICC%20Data%20Protection%20Principle%20of%20Accountability%20Discussion%20Paper.pdf

It is clear from the above that cloud service customers, and to a lesser extent; providers, are already operating in an environment that is highly regulated. As a result, calls for further regulation of the cloud computing market should be viewed in this light.

The case for flexible and light touch regulation for emerging and innovative technologies and business models

As stated earlier, the near term objective for regulators should be a consideration of how to apply existing regulation to the cloud environment. Where gaps are found, a flexible and light touch approach to regulation is advised.

Where additional regulation is needed, and if applied in a sensible manner, it could have a positive effect on the market by providing cloud customers with additional confidence thus driving greater take up and adoption. The regulatory issues identified above are closely matched to the practical and commercial concerns of cloud customers outlined earlier in this statement and, to an extent, cloud providers. Concerns about security and control of information are one of the major barriers to the take up of cloud services so it is in all parties' interests to ensure these issues are addressed in a sensible and coherent manner. The current regime allows customers to contract for Cloud services safely without the need for further regulation; indeed customers have done so successfully for many years already in some areas. **Governments' and regulators' role in the cloud market, should therefore be largely to encourage, to dismiss unfounded concerns, to monitor the evolving market, and where necessary, to take action against service providers who seek to exploit customers fraudulently or unduly constrain competition.** In turn, it is important that all providers of cloud services have appropriate policies and practices in place that: are compliant with applicable laws, are consistent with relevant industry best practices and use meaningful and reasonable efforts to address and deter the use of their services to engage in illegal activity.

Conclusions

Although cloud computing offers new opportunities, for both buyers and sellers of services, the practical risks faced by businesses and consumers when dealing with cloud based services are not new. Business has faced these challenges – the location of information, security controls over their information, the consequences of exiting a commercial arrangement and so on – in outsourcing arrangements for many years.

For the same reason, cloud computing does not pose major new regulatory challenges, On the contrary, cloud services are already subject to a wide variety of extensive regulatory regimes. In many cases, the outsourcing industry has evolved solutions to the regulatory and commercial challenges these regulations raise which balance customer needs and cost. By applying those solutions, customers can today contract with confidence with cloud service providers. At the same time, governments should be encouraged to exercise the regulatory powers they have, in the fields of consumer contracting, advertising and trading standards and privacy notably, in order to ensure that the credibility of the cloud market is not harmed by 'rogue providers' of cloud services.

:-:-:-:-:-:-:-:-:-:

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 the Digital Economy

Business leaders and experts develop and promote the continued and stable growth of the digital dconomy, and further adoption of its underlying Information and Communication Technologies (ICT) foundation, through regulatory advocacy of key business positions and best practices through ICC's Commission on the Digital Economy.

Through its members who are ICT users and providers from both developed and developing countries, ICC is recognized in expert circles as the global consensus voice for private sector expertise on policy matters that drive the Digital Economy. It also provides the ideal platform for developing global voluntary rules and best practices for this area of interest to companies worldwide. Dedicated to the expansion of secure ICT-facilitated trade, ICC champions the liberalization and regulatory harmonization that are required to achieve a free flow of information across all borders.

ICC led and coordinated the input of business around the world to the United Nations World Summit on the Information Society (WSIS), 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).

International Chamber of Commerce
The world business organization
Policy and Business Practices
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