United Nations A/CN.9/856

General Assembly

Distr.: General
5 June 2015

Original: English, French and Spanish

United Nations Commission on International Trade Law
Forty-eighth session
Vienna, 29 June-16 July 2015

Possible future work in the area of electronic commerce — Contractual issues in the provision of cloud computing services

Proposal by Canada

Note by the Secretariat

The Secretariat received the proposal by Canada (in English, French and Spanish). The text received by the Secretariat is reproduced as an annex to this note in the form in which it was received.

V.15-04050 (E) 120615 150615

Annex

CONTRACTUAL ISSUES IN THE PROVISION OF CLOUD COMPUTING SERVICES GOVERNMENT OF CANADA

I. Foreword

1. At its forty-seventh session, in 2014, the Commission received two progress reports from Working Group IV on Electronic Commerce about its work on model provisions for electronic transferable records. Given the progress accomplished on the model provisions, the Commission was asked to consider future work in the field of electronic commerce which would be undertaken after the forty-eighth session of the Commission, when the current mandate of Working Group IV is completed.

2. In that context, the Commission took note of a proposal by the Government of Canada with regards to legal issues on cloud computing (A/CN.9/823). It was explained that the proposal was intended to request the Secretariat to gather information relating to cloud computing and to prepare a document identifying potential risks stemming from current practices in relation to conflict of laws, the lack of a supporting legislative framework, and the possible disparities in domestic laws.

3. There was wide support for that proposal recognizing the implication of cloud computing, particularly for small and medium-sized enterprises.[1] However, it was suggested that caution should be taken to avoid engaging in issues such as data protection, privacy and intellectual property, which might not easily lend themselves to harmonization and might raise questions as to whether they fall within the mandate of the Commission. It was also stressed that work already undertaken by other international organizations in this area, by the OECD and APEC for example, should be taken into consideration so as to avoid any overlap and duplication of work. It was also suggested that a compilation of best practices might be premature at the current stage. Subject to those comments, it was generally agreed that the mandate given to the Secretariat should be broad enough to enable it to gather as much information as possible for the Commission to consider cloud computing as a possible topic at a future session.[2]

4. With the view of providing assistance to the Secretariat in its preliminary work on the subject, Canada has prepared this document to underpin the relevant issues for review by UNCITRAL. The document was prepared in consultation with experts in the field and expands on the issues identified by the Canadian proposal in relation to the provision of cloud computing services.

---

[1] A/69/17 — Report of the United Nations Commission on International Trade Law, forty-seventh session (7-18 July 2014) , at paragraph 147.

[2] Idem, paragraphs 147 and 150.

Part I: Cloud computing, risks and benefits

A. What is cloud computing?

5. Cloud computing can generically be defined as computing services (e.g., data hosting or data processing) over the Internet.[3] It requires some form of controlled access to the computing functions, such as restricting access to the employees of a business. What is often difficult for the layman to conceptualize is that it involves a variety of configurations of computer hardware (or group of computing hardware) called servers. Physically, the pool of hardware resources is provided by several servers and networks located in various places. Typically, once individual users have been granted access, they can use the servers' processing power to run an application, store data, or perform other computing tasks. It is described as a "cloud" because computing functions are not performed exclusively on a personal computer, but elsewhere on servers through an Internet connection.

6. The span of cloud computing services available in a given location can vary because local applicable laws (e.g., government regulation of personal information held by public entities) require data to be physically hosted in specific locations, often within the jurisdiction of the service applicant, or because of the quality of the information and communication technology infrastructure that is available in that given location. In the majority of jurisdictions, there are limited restrictions imposed by law or by the local infrastructure and the limits that exist usually stem from how much the customer is ready to pay or from the inability of potential clients to fully grasp the potential cloud computing represents for them.

7. Cloud computing features are: on-demand self-service, network accessibility, resource pooling, elasticity and scaled service. On-demand self-service means that the service is available at any time on demand and without the need for human involvement by the service provider. Network access usually means that the cloud is available through Internet connections. Pooling means that the computing capacity of the service providers are not attributed specifically to each user, but that computing resources of the service provider are available for use in their unlimited capacity to all users. This latter aspect is referred to as the elasticity of the service. Services are scaled and adapted to the needs of each client, large or small.

8. From an economic perspective, cloud computing provides the ability to access IT resources on demand without the need for significant capital expenditure. It thereby significantly lowers upfront capital investment required from small businesses. Cloud computing is thus an important element for businesses in obtaining a competitive advantage or to be on a level playing field with other market participants. Cloud computing itself is a new form of IT activity and recent figures show that it is becoming an important sector of business activity.[4] Beyond that, one must recognize that innovation is likely to be stimulated by cloud computing platforms as was the case in recent decades for other forms of IT solutions. Cloud computing facilitates online collaboration on a global scale which

---

[3] The provision of cloud computing services is not restricted to online Internet but can also be offered on closed network.

[4] World Economic Forum, "Advancing Cloud Computing: What to Do Now?, Priorities for Industry and Governments", 2011, p. 1.

is recognized as a tool facilitating innovation and economic growth.[5] By leveraging cloud computing solutions, SMEs save on investment costs and, at the same time, benefit from gaining access to cutting edge technology and services, including software updates.

9. From a technology perspective, while cloud computing technology is widely available and used in developed countries, important challenges still need to be overcome for similar level of cloud computing technology to be widely accessible in many developing countries. In particular, the availability of broadband network infrastructure remains a challenge in many developing countries or the cost of access to broadband network is comparatively high for local businesses in these countries. The role of policymakers in fostering broader access to cloud computing and the advantages for developing countries of cloud computing have be reviewed by a number of development organizations.[6]

(a) Various existing models and characteristics

10. Given the wide variety of services offered and the technologies used to deliver the services, it is useful to categorize existing forms of cloud computing.[7] Typically, cloud services are divided into three categories[8] varying from the supply of "raw" computing capacity to an "off-the-shelf" software:

(i) Infrastructure as a service (IaS)

11. IaS is the provision of cloud services where an organization outsources the resources and equipment used to support virtually any computing operations such as virtual server space, network connections, bandwidth, IP addresses and load balancers (a computer networking process distributing workloads across multiple servers). The client is given access to the various components online in order to build its own IT platforms. This service is often used by enterprises and is paid on a per-use basis.

(ii) Platform as a service (PaS)

12. PaS is a category of cloud computing service that provides a platform and environment to allow developers to build applications. It allows users to create software applications using tools supplied by the provider. Depending on the service providers and the sophistication of the client, PaS services can consist of

---

[5] OECD, "Cloud Computing and Public Policy", Briefing Paper for the ICCP Technology Foresight Forum, 14 October 2009, para. 4.

[6] Cloud computing provides a very effective means for organizations and consumers in developing countries to access powerful computing resources at low cost. However, some challenges must be addressed by policymakers: (i) expanding fixed and wireless broadband access in developing countries; and (ii) spurring the development of cloud computing to take advantage of cloud computing resources to stimulate economic growth and enhance educational capabilities. See UNCTAD, Information Economy Report 2013, "The Cloud Economy and Developing Countries", 2013.

[7] This text does not deal with the distinction between public and private clouds because it would go beyond the scope of this preliminary analysis. It is however acknowledged that public clouds often bring risks that can be systemically different from the relative secure private cloud.

[8] OECD, "Cloud Computing and Public Policy", Briefing Paper for the ICCP Technology Foresight Forum, 14 October 2009, para. 16.

preconfigured features that can be selected on the basis of the client's requirements. It can also consist in the provision of packages of services or applications depending on the needs or the expertise of the client.

(iii) Software as a service (SaS)

13. SaS is the category of cloud computing services most typically used by individuals for personal needs. Consumers are able to access software applications over the Internet, which are readily accessible and usable for personal consumption. Google and Microsoft Office are examples of SaS. Business can also use SaS for a broad range of needs, including accounting and invoicing, sales numbers monitoring and tracking as well as the communications generally (Internet presence via existing platforms and e-mail messaging systems). SaS is essentially a form of software-on-demand. Instead of purchasing software for installation onto computers or networks as traditionally done, software applications of the service providers are accessed. SaS users therefore do not need to acquire specific software and are not responsible to pay the corresponding IP rights.

B. Benefits of using the Cloud

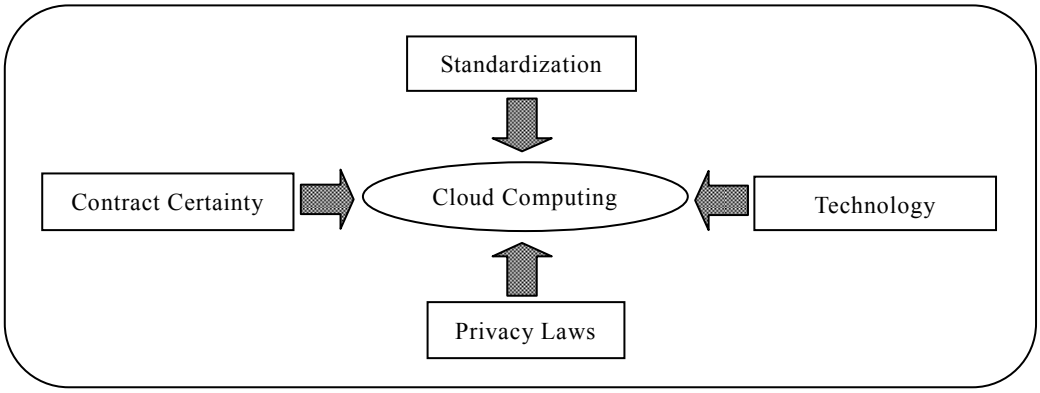
14. The benefits of using cloud computing are multiple and for each business will depend on its activities and on whether cloud computing can contribute to lowering the cost of the goods or services it produces or to marketing its products more effectively. The benefits can range from increased security and user friendliness to cost savings and the creation of innovative new products and new market opportunities. What is important in order to fully assess the impact of the Cloud on international trade is the economic spin-off that results from cloud computing and the impact at a macroeconomic level on businesses. Cost savings and the opportunities for innovation that cloud computing brings to small and medium-sized enterprises stand out as important benefits.

15. More generally, it has been said that the economic benefits at the microeconomic level of using the Cloud are: an increase in productivity, economies of scale, reduced operating costs, reduced capital expenditures, greater access to markets in a time efficient manner, increased leverage through the use of an organization's information and data, improved IT security, new business opportunities, reduced initial capital investment for start-up businesses and a positive effect on entrepreneurship.[9]

16. From a macroeconomic perspective, the development of cloud is a function of four key factors: the availability of technology; contractual predictability and certainty surrounding the use of cloud; the existence of standards allowing, among other things, the interoperability of the cloud products and interfaces as well as better definition of the service provided; and the existence of adequate legislation on privacy and on the protection of confidential information. These factors are illustrated in figure 1.1 (below).

[9] ICC, Business views on regulatory aspects of cloud computing, February 2012, p. 4.

Figure 1.1
Key elements for a conductive cloud computing environment



17. An optimal environment will be found in a jurisdiction where all four factors are present. Jurisdictions performing well in terms of making these four factors available will be creating an environment favourable to the Cloud and therefore to commerce. The availability of a good cloud environment domestically will facilitate the emergence of competitive local businesses which will in turn offer goods and services at competitive prices on international markets.

18. Legal issues affecting cloud computing are not assessed from the standpoint of necessarily creating an incentive for business to seek cloud computing solutions, but rather to review whether the legal environment, because of its deficiencies or because of unnecessary legal restrictions, does not allow cloud computing-related benefits to be fully unlocked. Indeed, the economics of a particular business sector and market forces should attract the required IT solutions. The legal environment should not be promoting nor impeding the adoption of IT solutions. It should be neutral, leaving businesses with the decision of what the best-suited IT solution is.

C. Risks associated with the Cloud

(a) General — Risk differentiation from traditional market conditions

19. The Cloud can be considered a form of outsourcing. For customers, it means that the risks that exist with any outsourcing are also present with cloud computing. For example, will the computing services received be adequate to support the enterprise's needs and to ensure that the enterprise's output quality is maintained? From the service provider's perspective, in addition to the risk associated with whether it can provide the services in accordance with the terms of the contracts, a number of other risks ought to be assessed prior to concluding the agreement. For example, what implied terms are there for this type of service? What happens in cases where the data is accidentally lost, service is interrupted for reasons outside the control of the service provider, or the service is used in the pursuance of the client's criminal activities?

20. Outside these common considerations for assessing business risks, there is a fundamental difference between the Cloud and the traditional manner of outsourcing services. The service is virtual; that is, there is no physical presence of the service

provider at the user's premises. To some extent, the service provider itself is virtual. While cloud computing does not create aggregate risks or undiversifiable risks (i.e., a risk vulnerable to events affecting aggregate outcomes such as broad market returns, which are caused, for example, by natural disasters), it does potentially create a category of transversal risks which are unique. The risks are transversal because the data off-loaded on the Cloud may cover a very wide range of the users' activities and, in most situations, the risks are further amplified because of the impossibility of knowing where the data is hosted or processed. This situation prevails because, under existing cloud computing models, data is regularly transferred across borders and processed in various locations around the world depending on the availability of computing capacity. Transversal risk factors are not always present in traditional business conditions, but are almost always a component of cloud computing services.

21. For the purpose of this analysis, economic, security and legal risks are the most relevant and therefore the subject of detailed analyses. It should be noted however that risks are difficult to categorize. A legal risk can easily represent an economic risk as well because of its potential financial impact on the business and its activities. Similarly, a security risk will also represent an economic risk. Environmental and social risks have not been assessed for the purpose of this analysis.

(b) Economic risks

22. The economic benefits of using the Cloud arise from economy of scale one can achieve by pooling computing resources within the control of one supplier who then offers them at discounted prices to multiple users.[10] Indeed, from an economic perspective, the risks with cloud computing include considering the opportunity cost of not using the Cloud. Maintaining networks, updating software and storage capacity, not to mention adequate security features, are all costly.[11]

23. Traditional economic risks that exist for outsourcing services are also present in the cloud environment. For example, outsourcing internal functions of a business on the basis of incomplete assessments as to the needs and the potential cost savings can result in financial losses. It cannot be said that cloud computing is always a better option. Cost-benefit analyses must be conducted. Needs and objectives must be established at the outset before outsourcing computing functions. The most common economic risks are: acquiring cloud computing services that are unsuited to the business needs or the business model, loss of productivity in the transition period or loss of clients not interested in updating their practices to meet the Cloud's requirements.

24. Data is often among a business' most valuable assets. Preventing its loss and the consequences of that loss are therefore key in limiting risks for a business. The risks increase when data is stored and transmitted via the Internet and not in closed systems. The growing use of cloud computing has contributed to increased data

---

[10] OECD, "Cloud Computing and Public Policy", Briefing Paper for the ICCP Technology Foresight Forum, 14 October 2009, para. 9; ICC, Business views on regulatory aspects of cloud computing, February 2012, p. 4.

[11] According to some sources, database management currently accounts for more than 25 per cent of most companies' IT budgets, The Global Information Technology Report 2012 , p. 91.

processing outside of the comparatively secure business premises. The risks also vary depending on the nature of the information that is contained in the data. Some of the most significant economic risks are: lost data; loss resulting from unauthorized use of data; business interruption or disruption of activities; breach of service agreements; and loss of revenues because of reputational damage.

25. Increasingly, businesses holding trade secrets or sensitive client information devote time and resources to the development of good practices in IT governance. IT governance falls under the mandate of a company's officers and the board of directors. Widely accepted practices on corporate governance now require IT risks and permanent monitoring and assessment to form an integral part of an organization's risk management plan. Their adoption and implementation fall under the purview of the board of directors and the corporation's officers. IT governance represents an expense for businesses which could be offloaded to cloud service providers at a lower cost. That being said, failure to adopt and implement adequate IT governance can expose the business to lawsuits if affected parties can demonstrate the business was negligent. Again, cloud computing might be part of the answer and represent a significant economic advantage for the businesses using it.

26. Moreover, cloud computing has made available efficient tools and processes to analyse data at a small cost and opens up the possibility of extracting important information from data (such as purchase patterns, geotagging, in-depth analysis of clients' behaviour through algorithms, etc.) resulting in business opportunities. The result is more productivity and greater competitiveness that create substantial economic and social value for companies, governments, and consumers. From an economic perspective, the opportunity cost for a business not to use cloud processing could be significant.[12] For example, for a small-sized enterprise, the inability to match its own business data, such as customer information, business cycles, or product specifications, to relevant business sector studies and surveys or analytical processing schemes can prevent a business from adapting sales and marketing strategies to match potential clients' needs in a manner that is available to others in the same business sector.

(c) Security risks

27. The security of cloud computing is an important differentiating factor among cloud service providers and plays a role in decisions to migrate information systems to cloud computing environments.

28. This risk assessment is dependent on the circumstances and the business that is considering using cloud computing as an enhanced IT system security. Some businesses, in particular small and medium-sized enterprises, may have unreliable computer systems and security protocols or may not have the proper staff to ensure the existing IT systems are used in a safe and appropriate manner.[13] For these

---

[12] Consider for example "Rewards and Risks of Big Data", The Global Information Technology Report 2014.

[13] For example, standard security protocols require that passwords be relatively sophisticated using a mix of alphanumeric characters with special symbols (e.g., #,$ or %). In addition, after a limited number of attempts with the wrong password, the access is locked. Businesses may exceed minimum security requirements considered adequate in their fields or be under protected.

organizations, the opening up of the IT system to the Cloud does not necessarily constitute an increased risk, but rather access to enhanced security. The benefit for any given organization of the enhanced security cloud computing can offer will depend on the nature of the information it holds. For businesses hosting limited sensitive information, cloud computing can also limit risks by closing access to forms of hacking which are not directed to obtaining confidential information, but merely to disrupting business activities by tampering with its IT capability.

29. The acquiring business must assess the IT solution chosen prior to entering into a contract. This requires an exchange of information between the service provider and the business. This information-sharing is crucial, but there is also a need to ensure that the cloud services client has the ability to assess the security level of the provider's environment. A lack of information sharing or the inability of the acquiring business to assess this information is a serious potential threat for clients using these services.

30. The security risks associated with cloud computing stem primarily from the following threats:

Loss of control — (i.e. a client's decision to migrate all or part of an activity to cloud computing implies relinquishing partial control to the service provider.) Once the data has been given to a cloud solution provider, it becomes difficult for the client to verify whether it is being handled adequately in terms of its processing or retention. This loss of control varies depending on the type of cloud service.[14] The loss of exclusive control may result in an inability to deploy the necessary measures to guarantee data integrity and confidentiality.

Service provider's inconsistent or inappropriate security practices — Related to the preceding is the risk associated with the provider's security practices. Inadequate practices will lead to more significant risks for the client receiving the cloud services. Some inadequate practices may be related to operations control, insufficient authentication procedures, unavailability of encryption or weaknesses associated with the data retention process.

Vagueness in sharing roles and responsibilities — Various stakeholders are involved in a cloud solution model: the service provider, the service consumer, the client's computer administrator responsible for client security, third parties whose information is held by the business, etc. Any ambiguity in defining the roles and responsibilities related to data ownership, access control, maintenance of infrastructure, etc. may result in security risks. The failure to clearly assign responsibilities will have a higher impact where a third party's servers are used.

Unauthorized access to cloud services — The program interface (API) is the software layer (middleware) between the infrastructure and the service user.

---

[14] For example, in the case of IaS, only the management of equipment and the network is delegated to the provider. Unless it is very specific about the type of infrastructure sought, IaS is the cloud service that offers the lowest degree of dependency. With respect to a PaS solution, the link between the use of the service and the technological platform of development ensures that data conversion or exportation is difficult. Risks are therefore in relation to the control as well as conversion and extraction of information. With respect to SaS, control over the applications as well as the other elements is delegated.

Particular attention must be paid to interface control processes when entering identification and authentication data. Remote connection provides opportunities for cyber pirate attacks such as interception of communications, including passwords, phishing, fraud and the exploitation of software vulnerabilities.

Cross-border data flows — Breach of data confidentiality is a common risk for users of cloud computing. The lack of information about where the data is located and hence the applicable legislation and regulations as well as the number of stakeholders in a cloud computing solution accentuates this risk. Protecting sensitive, personal data as well as respecting the right to privacy is particularly difficult in infrastructures that are shared and potentially accessible to local governments. This situation also brings jurisdictional issues given the location of the data.

Data preservation — Data preservation includes a set of risks in relation to the loss of data, but also in relation to maintaining the integrity of the information. In addition, electronic documents often require that specific measures be taken regarding data integrity in order to be admitted in evidence. Cloud computing may accentuate the difficulty of taking adequate measures on this point. Some customers may require to have the ability to obtain evidence of satisfactory data protections through periodic audits.

Loss or disclosure of information — The loss of an encryption key or a user access code is one of the common risks associated with causing the loss or disclosure of information. A common feature is for the service provider to notify the customer of accidental disclosures of information when known.

Insufficient silos in shared environments (permeability) — The organization of cloud based resources allows different cloud service consumers to share the same infrastructure. The primary concerns stemming from this organization are related to silo architecture, isolation of resources and data segregation. Cloud computing in a public or semi-private form shares the services offered to the entire client base, creating a risk of data permeability among the various clients.

Unauthorized access during hosting and processing — Virtualization technology is the basis of cloud infrastructures. Hypervisors manage virtual functions co-hosted on the same physical server by sharing of the central processing unit and memory. The failure to prevent hypervisor attacks causes unauthorized access to the memory of the various virtual functions, which would otherwise remain separated, and jeopardizes the entire infrastructure.

Delegation of governance — IT governance falls under the mandate of a company's officers and the board of directors. Their adoption and implementation fall under the purview of the board of directors and the corporation's officers. A risk with the use of cloud computing solutions is that responsibilities in relation to the IT governance end up being partly delegated to the cloud service provider.

31. Given these cyber risks, there is a demand for insurance coverage for the exposure to potential losses of companies. The complex and somewhat evolving nature of cyber risks means that highly specialized expertise and experience are

needed to develop models for new insurance products to adequately cover these risks or that insurance costs are high.[15] The cost of these insurance products is passed on to businesses and consumers.

(d) Legal risks

32. The legal risks associated with a commercial venture can only be adequately assessed if the matter which is the subject of the contract is known (or can be known if questions are being asked and answered adequately). An added difficulty caused by the novel nature of cloud computing is that a prospective cloud customer, or his counsel, may not always be in a position to readily assess or determine the issues that need to be considered and, therefore, the questions to ask or the requirements to be requested from the service provider.

33. In recent years, the emergence of "international standards" put forward by trade associations and non-governmental membership organizations have contributed to addressing and limiting legal risks associated with the Cloud. These standards are incorporated by reference in contracts between the cloud service provider and customers and represent an off-the-shelf solution to a number of cloud computing risks.

34. The following paragraphs describe the legal risks from the perspective of each cloud computing participant. It goes without saying that many of these risks are similar to those of any contractual dealings, but IT services are somewhat of a different category because of their nature. The breadth of services covered — from advertisement and public presence on the Internet to the management and protection of confidential information — are such that they are services used as input in the provision of goods or services unlike any others. They are also used by all spheres of business and government activities. These services are far more than mere input used in production: they also involve the protection of confidential information and business secrets as well as the image of the business and are the general records of all the activities of the business.

(i) For cloud service providers

35. Entering into a contract for service for a cloud computing supplier will entail varying levels of risks and difficulties. Standardized services, typically with respect to SaS agreements, will be less risky and relatively easier to negotiate, because they will involve a common contract with standard clauses.

36. In other situations, for example when contracts are customized to the needs of a specific client, the legal position of the cloud provider will be different. Negotiations with the customer will require more care and considerations of the legal implications of the contracts.

37. Typically, two broad categories of risk will be assessed by the service provider: first, the risks linked to inadvertent or illegal release of confidential or secret information of the client and second, the risks associated with a failure in the provision of the services, such as interruption of cloud computing services or

---

[15] World Economic Forum, "Advancing Cloud Computing: What to Do Now?, Priorities for Industry and Governments", 2011, p. 10 and 14. Insurance products were referred to as being underdeveloped.

connectivity and loss of data. In both of these categories, the risks may stem from the actions or omissions of the service provider or from circumstances outside of its control. These risks can be limited by exclusions in the service agreement or by the taking up of insurance covering these specific risks.

38. Service providers will often be familiar with one or some limited number of local laws and in particular local contract laws and privacy laws. They will therefore either choose an applicable law that provides requirements in terms of protecting the confidential information that it can meet — or that it is willing to meet — and that offers rules of construction of contracts that are predictable and acceptable for its purposes. For example, a common law concept in the interpretation of contracts is that there may be "implied terms". Courts find that in certain circumstances everything agreed by the parties is not contained in the document and some additional terms must be implied. An implied term could for example be the obligation to proceed with the utmost care with confidential and sensitive information. Similarly, a civil law jurisdiction could have specific rules of interpretation of contract which state that any ambiguity in the contractual terms ought to be interpreted against the party who drafted the terms.[16]

39. There are limits to the effects of a clause on the selection of the applicable law. First, the parties may have derogated from the applicable law by agreeing to specific terms in their agreement. Second, there may be mandatory provisions of laws that apply regardless of the existence of a clause on the applicable law. Third, the rules on jurisdiction of domestic courts and the existence or absence of a clause on jurisdiction in the contractual agreement can also affect the determination of the obligations of the parties. In some circumstances, a domestic court may choose to disregard foreign law and apply its own rules. This could be the case, for example, if foreign law is not pleaded or insufficient evidence on the content of foreign law is brought to the attention of the court.

40. A fundamental difficulty in assessing the legal risks in a contractual agreement for the provision of cloud computing is that, in a cross-border situation, beyond contractual terms agreed by the parties, a number of laws can apply even in the presence of a clause on governing law.

(ii) For cloud service applicants

41. In the majority of situations, the cloud service applicant will be the weaker party or will be presented with a standard contract whose terms will not be open to negotiation. This will often be the case when dealing with SaS. In many situations where IaS agreements are negotiated, the parties are on a level playing field because they will both be knowledgeable about the risks and the implications of the terms of the contract. Where an imbalance between the parties exists, applicable contract laws will often provide that the contract is a contract of adhesion.

42. The most important legal risk for applicants remains not being in a position to fully assess the risks associated with the cloud computing agreement (e.g., inherent weakness of the technology being used, absence of or inadequate security features, economic risks linked to data loses or breaches, etc.). This incomplete assessment

[16] This will be the case when the contract is considered to be a contract of adhesion for example.

leads to inadequate terms in the contract or the absence of terms addressing specific risks.

(iii) For users

43. Users will not always be party to the cloud contractual agreement. For example, an employee of an enterprise who uses the Cloud in his capacity as employee will not be party to the contractual agreement between his employer and the cloud service provider.

44. Inappropriate use of the Cloud by an employee resulting in financial losses for the employer will usually be sanctioned according to the employment contract or the applicable contract law. The employer might be well advised to consider whether the contractual terms it uses for employment purposes are adequate to deal with reckless or ill-intentioned employees. This will be a risk for the employer because third parties will generally be seeking redress from the legal entity tasked with protecting the confidential information rather than its agent. However, if an affected third party can identify wrongful or malicious actions by an employee or agent (considered as user here) of one of the parties to the cloud computing agreement, it is possible under some systems of law to seek redress by suing the employee or agent.

45. Although this will generally not be the case under a typical cloud computing agreement, employees or agents may have personal information, proprietary rights over property, or trade secrets that are covered by the data falling under the Cloud. For example, a university enters into a cloud computing agreement for its general computer needs, including messaging, payroll and data bases, where professors save their research projects. These projects may in whole or in part belong to the professors. In this situation, a user of cloud solutions, who is not a party to the cloud computing agreement, could be affected by mishandling of data by the service provider or the university.

(iv) For third parties

46. Third parties are not directly affected by a cloud computing agreement. They are not party to the agreement. Because of the rule on the privity of contract, they only have effects among the parties. Therefore, third parties cannot require that any aspect of the cloud computing agreement be executed. For example, a third party could not exercise a contractual remedy against the cloud service provider for the failure to ensure the protection of its personal information.

47. Third parties might nonetheless be affected by practices resulting from the cloud computing agreement. Recourse against the cloud service provider will generally have to be sought through tort remedies or through legislative provisions allowing recourse against a faulty party, for example when it did not use reasonable care to protect the third party's information. However, knowing this possibility of extra-contractual claims, can the service provider limit its potential liability contractually? One manner of achieving this objective is by subscribing risk insurance covering claims from third parties in given circumstances where data was misused, lost or misappropriated.

Part II: Consideration of legal issues

A. Categories of cloud computing contracts

48. The traditional categories of cloud computing services have been described as SaS, PaS and IaS. These categories reflect the practical and technology-oriented use of cloud computing. Although relevant to the legal analysis, these categories are incomplete because they fail to identify legally relevant factors such as the creation of protected IP rights and proprietary rights. Contracts covering cloud computing services can be categorized in four groups:

(a) Common text processing and mail services;

(b) Data hosting (protection and preservation of data);

(c) Use of licensed software or database and other protected IP rights;

(d) Proprietary work product (i.e., work product resulting in shared or partial ownership of product).

49. From a legal standpoint, all four categories of contracts entail different considerations for the parties and different legal consequences. The first category is commonly used by individuals for personal needs. Contracts for office-based services of cloud-based services (e.g. e-mail, word processing, minimal storage of information, etc.) are generally basics and rely on widely available technologies and software which can be accessed using commonly available mobile devices and at low costs. Because of the scale and of the standardization of the services provided, there is often very little opportunity to negotiate agreements individually. In a business setting, this computing solution can be considered useful, for example for communications purposes, while the protection and preservation of confidential information are provided in-house.

50. In the traditional office context, companies and users rely on the integrity of their hard drives and related back-up systems. These systems are governed by warranties that may guarantee the replacement of the hardware, but usually do not 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, 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. The second category therefore involves storage capacity coupled with corresponding security features for data preservation and limiting access to authorized users. There are obviously varying degrees of sensitivity of confidential information.

51. The third type of contract involves the use of licensed material. This will often be the ability to use databases. A number of professional service providers, for example, use databases to extract information or to proceed to analyses which are subsequently incorporated in the service provided. This type of contract therefore covers both the ability to use IP-protected information and to disseminate part of it in the output of the subscriber. At times, the IP owner will require as part of the terms and conditions that reference be made to the IP owner in the output of the users.

52. The three types of contract described so far are generally SaS contracts. They generally involve limited work product that is IP-protected. The fourth type of contract results in an integrated use of the computing resources of the service provider as well as the input of the user, which become part of the output. The fourth category entails the creation of work product and associated proprietary and intellectual property rights. A lack of standards and a lack of widespread adoption of existing standards in the case of platform as a service (PaS) can create a situation where the output cannot be used without the application programming interfaces (APIs). It means that applications or products developed on one platform cannot easily be migrated to another cloud host or be used on any computer. As a consequence, once an organization has chosen a PaS cloud provider, it is locked-in. In some situations, the output can essentially not be used without prior consultations with the rightful proprietary owner of the platform. Promoting open standards for APIs and further work on interoperability could limit the situations where proprietary rights can be asserted by cloud providers.

53. While some providers, in particular large ones, can do little to customize mass offerings beyond providing menu-driven choices (e.g., "web wrap" and "click through" agreements found on websites for cloud services with standard security features), customers should be mindful that the four types of contracts entail different consequences which need to be carefully assessed at the outset.

54. Most cloud computing services will contain some features that can be associated with one or more types of contract. Note that the delivery of cloud computing solutions varies constantly and these models are evolving, are not always fully demarcated and may overlap.

B. Contractual issues

(i) Application of private international law criteria

55. The law applicable to contractual obligations is the law selected by the parties, unless the particular contract falls under a category for which rules of law impose a specific applicable law (e.g., in some aspects relating to family property). Provided the intention expressed is bona fide, and provided there is no reason for avoiding the choice on grounds of public policy, the intention of the parties as to the choice of law prevails.

56. In the absence of a choice of law by the parties, the intention of the parties will be ascertained by the intention expressed in the contract itself or, in the absence of such express indications, the proper law will be determined by inference from the terms of the contract and the surrounding circumstances (which latter connecting factors are known as the law that has the "closest and most real connection" with the transaction). However, traditional factors may not be readily identifiable for a given cloud computing contract. For example, where was the contract negotiated and signed in a virtual environment? Where is the contract expected to be performed? Where is the cloud computing service provider located?

57. These issues are of limited application to the extent that the vast majority of cloud computing contracts do provide for a choice of law. However, should there be

some guidance for cases where the parties accidentally or knowingly did not select a governing law? Should there be limits to the choice of governing law?

(ii) Limitations on movement of data and control over data

58. While in traditional contracts for service, it is relatively easy to determine whether a contract has an external element. Cloud computing will often entail an international component because data will often be stored or will transit between servers located in different countries. Indeed, from a legal risk assessment perspective, parties to a cloud computing agreement and their counsel should expect an international dimension to be present.

59. Cloud computing agreements can be domestic, which means the contract, the parties and the performance of the obligations, are domestic in all respects. They can also involve a foreign element, in which case it is possible for the agreement or the legal relationship to be affected by multiple laws and for more than one court to have jurisdiction to hear disputes in relation to the contract.

60. One solution to this problem is to require that the data be retained within the jurisdiction at all times. When considered desirable, parties to a cloud computing agreement may request that data be physically stored within a specific jurisdiction with the objective of ensuring a single local law applies to the cloud computing agreement, the parties and the data. This approach has been advocated by some governments where satisfactory protections are not able to be put in place and in order to avoid the application of foreign laws to the data contained in the Cloud. However, no contract, no matter how well drafted, can completely exclude the application of a country's laws.

61. A permutation of the above practice is to require that information transmitted outside the jurisdiction be encrypted. This clearly brings up the question of whether the encrypted information is subject to the other country's law and, if so, what practical effect this has. This practice raises the question of whether a court in the jurisdiction where the data is located may require the disclosure of the encryption key.

62. In civil and commercial matters, courts can issue an order for the production of documents actually in the possession and control of a party to the dispute. Should a cloud service provider be required to produce electronic documents falling under its control? If not, is domestic legislation providing clear guidance to that effect? Is this situation exacerbated in cross border situations?

(iii) Duties and responsibilities of each participant to cloud agreements

63. What are the duties of the parties to a cloud computing agreement? Do they include the obligation to preserve data and redundancy? Are the parties limited to duties specifically mentioned in the cloud agreement? Do cloud service providers have the obligation to perform the contract according to recognized business practices and if so, what is the content of these practices?

(iv) Allocation of obligations, risks and liabilities under the contractual framework

64. In general, the respective obligations of the parties are laid out in the contract governing their relationship. Data storage and transfers from one jurisdiction to

another as part of resource management often result in challenges and risks which cannot be easily allocated at the outset. The jurisdiction where the server on which data is stored is not known to the cloud user and, as a result, the customer and the service provider have difficulty in thoroughly checking and controlling the data handling practices and in ensuring compliance, not only with the terms of the contract, but also with the various laws that can apply. Parties can provide specific checks and rely on validations processes to determine where data is located.

65. In the absence of any term in the contract for service, a person contracting to do work and supply materials warrants that the materials or services will be a sufficient quality and reasonably fit for the purpose for which they are contracted, unless the circumstances of the contract are such as to exclude any such warranty. Are there implied terms under a cloud contractual relationship? For example, does the cloud service provider warrant that it will comply with any applicable local laws where the data could be located? If the parties agree that the data should be hosted in specific geographic locations, does the cloud service provider warrant that it will be the case and that servers used for storage or computing purposes will be located exclusively in the designated jurisdiction?

66. Is it an implied term of the contract that the cloud provider is required to maintain control over data?

67. Are limitations of liability for data losses or corruption enforceable or are they considered unconscionable or unenforceable because contrary to the purpose of the contract?

(v) International standards incorporated by reference in cloud computing agreements

68. The emergence of “international standards” put forward by trade associations and non-governmental membership organizations may have contributed to addressing and limiting risks associated with the Cloud in particular for small and medium-sized enterprises which may not always have the resources or the expertise to consider all possible cloud-related issues. Should UNCITRAL consider whether such standards can be incorporated into best practices? Are these standards referred to in contracts between cloud service providers and customers effective and binding in the various systems of law?

(vi) Data hosting and proprietary rights

69. In many systems of law, the public and peaceful possession of personal property amounts to a presumption of ownership. Does this presumption cause difficulties in the world of cloud computing? Is the cloud service provider in possession of the data of its customers? What happens in situations where the proprietary rights over data or software have not been clearly established by the parties to the cloud agreement in particular in situation where IaS is being supplied?

70. Given the proprietary rights of customers over data maintained by the cloud service provider, should the service provider be required to surrender data to its legitimate owner upon demand? Would this obligation also include the obligation to erase or otherwise eliminate any back-up copies of the data?

(vii) Intellectual property

71. A number of clauses developed by cloud service providers specify that the client retains its intellectual property rights over the content of the information transferred to the provider. Sometimes, however, the provider gives itself a licence, sometimes universal and unlimited, to use, host, store, reproduce, modify, communicate and distribute the content.

72. Compliance with intellectual property rights is another issue that the client should be concerned about. Because of the nature of the Cloud, in some cases it can result in hosting being done in various and sometimes unknown locations. In that context, it could be difficult to predict what laws will be applicable given that intellectual property rights are often defined by reference to the laws in the jurisdiction. In addition, what constitutes a violation of copyright in one country may not be in another.

73. Determining the owner of the copyright where new works have been created in the context of cloud services is also an issue that can be considered.

(viii) Jurisdiction

74. What constitutes a sufficient connection to a given jurisdiction for a court to entertain a contractual claim arising out of a cloud computing agreement? To what extent should an exclusive choice of jurisdiction be recognized and enforced?

75. In the absence of a clause on jurisdiction where can the parties to the contract bring an action or seek provisional protection measures? What should be the basis for such exercise of jurisdiction?

Conclusion

The information provided in this note is aimed at advancing the review of legal issues affecting the provision of cloud computing services so that a Working Group can use this preparatory work in developing recommendations. The Commission may wish to acknowledge the issues raised in this note and mandate a Working Group to review these issues, as well as others identified in the course of its deliberations, and to recommend best practices where needed based on evidence of absence of legal recourses, perceived imbalance between the rights and obligations of cloud computing participants or other evidence. The Secretariat in order to assist the Working Group could conduct research on contractual issues that arise in the provision of cloud computing services and explore possible solutions in relation to some or all of these issues with the view of fostering international trade. Experts meetings and consultations could also be used to gather additional information.

Annex I: Current issues in cloud computing

76. International organizations have covered a wide-ranging number of issues relating to cloud computing. Their analyses constitute a matrix of information helping to understand and develop cloud computing and assist in delimiting critical legal issues in relation to the provision of cloud services.

(a) United Nations Centre for Electronic Business and Trade Facilitation (UN/CEFACT)

77. The UN/CEFACT, a subsidiary body of the United Nations Economic Commission for Europe (UN/ECE), supports activities dedicated to improving the ability of business, trade and administrative organizations, from developed, developing and transitional economies, to exchange products and relevant services effectively. The principal focus is facilitating national and international trade transactions through the simplification and harmonization of processes, procedures and information flows, and so to contribute to the growth of global commerce. A number of specifications and standards have been endorsed by CEFACT such as the ebXML global standards for exchanging business messages, establishing trading relationships, communicating data in common terms, and defining and registering business processes. The endorsement of these standards or processes can impact business practices and limit the issues of interoperability, and ultimately litigations.

(b) World Customs Organization

78. The World Customs Organization (WCO) is the only intergovernmental organization exclusively focused on customs matters. The work of the WCO covers the development of global standards, the simplification, harmonization, and modernization of customs procedures (including promoting the utilization of IT methods), trade supply chain security, international trade facilitation, the enhancement of customs enforcement and compliance activities, anti-counterfeiting and piracy initiatives, public-private partnerships, integrity promotion, and sustainable global customs capacity-building programmes. The WCO also maintains the international Harmonized System goods nomenclature and administers the technical aspects of the WTO Agreements on Customs Valuation and Rules of Origin. Additionally, the WCO and UNCITRAL are cooperating, with other international organizations, in a major programme to address the global legal issues related to the international Single Window.

(c) UNCTAD

79. The United Nations Conference on Trade and Development has developed considerable expertise in the customs area within its mission related to trade development. Numerous countries and economies have implemented its Automated System for Customs Data (ASYCUDA).

80. In 2013, UNCTAD released the *Information Economy Report, The Cloud Economy and Developing Countries*, which takes stock on the development of cloud computing in developing countries. It reviews the conditions required to foster the cloud computing economy and stresses the consequences for failing to do so. This document is seminal, in particular because of its approach to the assessment of what

the cloud computing economy is, as well as what ought to be considered in terms of infrastructure, policy and action to develop this field.

(d) International Chamber of Commerce

81. The International Chamber of Commerce (ICC) is the international private sector body that represents the interests of the global business community. The goal of the ICC is stimulating the global economy by setting rules and standards, promoting growth and prosperity, and spreading business expertise. The ICC has developed a range of Model Contracts and Agreements that cover the business components of the supply of goods as part of an international sales contract, for example its Model International Sales Contract, Model Commercial Agency Contract and Model Distributorship Contract.

82. The ICC Commission on the Digital Economy has recently published a paper reviewing the *Business Views on Regulatory Aspects of Cloud* recommending that governments be encouraged to use the regulatory powers they already possess in order to improve trust and understanding in the cloud services market. The paper concludes that risks faced by businesses and consumers when dealing with cloud-based services are generally the same as those faced in more traditional communications and business environments.

(e) The Organization for Economic Cooperation and Development

83. The Organization for Economic Cooperation and Development (OECD) is an international body comprised of 30 member countries. The goals of the OECD are to support sustainable economic growth, boost employment, raise living standards, maintain financial stability, assist the economic development of other countries and economies, as well as to contribute to growth in world trade. Important contributions have been made in relation to cloud computing by the OECD, in particular with respect to recommendations and best practices in e-commerce:

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Security Guidelines) (2002)
- OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication (2007)
- OECD, Cloud Computing: The Concept, Impacts and the Role of Government Policy (2014)

The most recent document, *Cloud Computing: The Concept, Impacts and the Role of Government Policy*, outlines possible government roles in terms of policies in relation to cloud computing.

(f) The Hague Conference on Private International Law

84. The Hague Conference on Private International Law is an intergovernmental organization whose purpose is to further the progressive unification of the rules of private international law. The results of its work include multilateral treaties in the fields of international legal cooperation and litigation and of international

commercial and finance law. Recent work at the Conference did not address cloud computing specifically. Existing conventions opened for signature and ratification may be relevant in the context of cloud computing, such as the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, the Convention of 1 February 1971 on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters and the Convention of 30 June 2005 on Choice of Court Agreements. In addition, the current work of the Hague Conference on a convention for the recognition and enforcement of judgements could impact cloud computing agreements and litigation.

(g) World Intellectual Property Organization (WIPO)

85. The World Intellectual Property Organization is a specialized agency of the United Nations. It is dedicated to developing a balanced and accessible international intellectual property (IP) system, which rewards creativity, stimulates innovation and contributes to economic development while safeguarding the public interest.

86. WIPO is consistently monitoring the application of existing international conventions protecting intellectual property in electronic commerce.

(h) Asia-Pacific Economic Cooperation (APEC)

87. The Asia-Pacific Economic Cooperation, or APEC, is a forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific region. APEC is an intergovernmental grouping that operates on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants.

88. APEC has long been committed to promoting Internet economy since the adoption of the APEC Blueprint for Action on Electronic Commerce at its annual Leaders' meeting in 1998 and the establishment of the APEC Electronic Commerce Steering Group (ECSG) in 1999, aiming to promote the development and use of electronic commerce by creating legal, regulatory and policy environments in the APEC region. In 2014, APEC continued to carry out work on promoting the Internet Economy by releasing the Concept Paper "Developing the Internet Economy through Enhanced ICT Cooperation" in Ningbo, People's Republic of China. The Data Privacy Subgroup (DPS) also reviews interoperability of the APEC and EU data privacy regimes.

(i) International Conference of Data Protection and Privacy Commissioners

89. The International Conferences of Data Protection and Privacy Commissioners bring together privacy Commissioners from countries around the world and adopt resolutions calling for best practices in the protection of personal data and confidential information.

(j) World Trade Organization (WTO)

90. The Declaration on Global Electronic Commerce adopted by the Second (Geneva) Ministerial Conference on 20 May 1998 urged the WTO General Council to establish a comprehensive work programme to examine all trade-related issues arising from global e-commerce. The General Council adopted the plan for this work programme on 25 September 1998, initiating discussions on issues of e-commerce and trade by the Goods, Services and TRIPS (intellectual property) councils and the Committee on Trade and Development.