United Nations A/CN.9/823

General Assembly

Distr.: General
20 June 2014
English
Original: English and French

United Nations Commission on International Trade Law
Forty-seventh session
New York, 7-18 July 2014

Planned and possible future work — Part IV

Proposal by the Government of Canada: possible future work on electronic commerce — legal issues affecting cloud computing

Note by the Secretariat

1. In preparation for the forty-seventh session of the Commission, the Government of the Canada submitted to the Secretariat a proposal in support of future work in the area of cloud computing. The English and French versions of that note were submitted to the Secretariat on 19 June 2014. The text received by the Secretariat is reproduced as an annex to this note in the form in which it was received.

V.14-04130 (E) 260614 270614

Annex

I. Introduction

1. Pursuant to the mandate from the 44th Commission Session in 2011, Working Group IV on Electronic Commerce (Working Group) has carried out its work on electronic transferable records, including certain aspects of other topics identified as warranting the attention of UNCITRAL, such as identity management, use of mobile devices in electronic commerce and electronic single window facilities.[1] For the 47th Commission Session, the Working Group will report on the work of its 48th and 49th Sessions. The work on model provisions for electronic transferable records is progressing. As such, it may be time for the Commission to consider future work in the field of electronic commerce.

II. Cloud computing and related legal issues in cross-border context

2. In recent years cloud computing has progressed rapidly and is now widely used in many sectors of business activities as well as by public sector bodies. Cloud computing can generically be defined as computing services (e.g., data hosting or data processing) over the Internet. It requires a form of restricted access which is granted to a defined group of individuals, such as 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. Individual users, once they have been granted access, can use the servers' processing power to run an application, store data, or perform any other computing task. It is described as "cloud" because the computing is not done on one's personal computer or on the business' own computer system, but elsewhere through an Internet connection. In effect, cloud computing limits the need for in-house computer networks, servers and even personal computers because instead of using these devices or in-house networks to perform computing functions, the applications and computing capacities of the service provider are used. Using cloud computing can greatly facilitate the conduct of business by reducing costs and increasing mobility of users.

3. Despite the advantages of cloud computing, businesses may be reluctant to use it because of issues of reliability, security of confidential information such as trade secrets, the absence of physical presence of the service provider in the jurisdiction, standard contract clauses perceived to be too slanted in favour of the cloud provider, the rigidity of the models proposed by service providers that are unable to satisfy legal requirements of the client, and many other reasons.

---

[1] *Official Records of the General Assembly, Sixty-sixth Session, Supplement No. 17* (A/66/17), para. 238- 239.

III. Why would work on identifying legal issues associated with cloud computing be useful

4. Given the importance of cloud computing in today's business world and its increasing use both domestically and in a cross-border context, it would be useful for UNCITRAL to carry out work on the legal issues affecting parties to a cloud computing arrangement. Outlining the legal risks associated with entering into contractual cloud computing agreements would be useful to private parties for the protection of their interests and in the assessment of how they carry on business. The consideration of cross-border cloud computing services by UNCITRAL would also contribute to the development of international trade by reducing or removing obstacles in international trade and by identifying opportunities for harmonization of practices and laws.

5. Cloud computing raises a number of contractual as well as other legal issues. Although intellectual property rights on software and privacy issues, including the determination of the applicable privacy law, have been identified and potentially create significant challenges in practice, the current proposal excludes intellectual property and privacy from the scope of the work proposed and is restricted to contractual issues affecting hosts, clients and users of cloud computing and related jurisdictional issues. It is limited to the preparation of a document outlining the cloud computing contractual relationships and legal issues that arise in that context. Without prescribing the form of such a document, it could be a checklist or a more detailed list of considerations for cloud users similar to other UNCITRAL documents in other fields, such as the *Notes on Organizing Arbitral Proceedings (1996)*, *Recognizing and Preventing Commercial Fraud: Indicators of Commercial Fraud (2013)*, or the *Legal Guide on International Countertrade Transactions (1992)*. The following paragraphs contain a list of issues that could be considered. The list is intended to be an illustration of the contractual aspects that could be considered and is non-exhaustive.

6. First, what are the duties and responsibilities of each participant to cloud agreements? Security standards of cloud providers are not regulated, depend on assertions that are difficult to verify for most clients and are supported by contracts that may be difficult to enforce in practice because of servers located in unknown places and interlinked with unknown servers. This raises issues about the compliance obligations to domestic laws, which in some cases might conflict. Can the duties and responsibilities be enforced and allocated in a cross-border context? What duties does the service provider have towards preserving the integrity of the data? What remedies are available in cases where the integrity of the data has been compromised? Can guidance be provided to service providers and applicants for the assessment and negotiation of contractual obligations? For example, what duties does the service provider have in relation to business losses due to the unavailability of the service? Under what terms can a cloud agreement be terminated? What happens to the data when the contract is terminated?

7. Second, secured access to cloud data hosting servers requires that adequate identity management protocols be established. It seems largely accepted that any identity management system is based to a large extent on a contractual framework. The contractual framework allocates obligations, risks and liabilities. However, is any contractual framework acceptable or should best practices be established? In

addition, how does States' domestic legislation apply to accepted identity management protocols? What do courts accept as reasonable practices and what do they consider being negligent practices?

8. Third, data hosting is governed by a contractual agreement between the service provider and the person, the applicant, wishing to make cloud data hosting available to a specific group of individuals (typically employees or clients). These contracts often contain standard terms from the service providers but may also be negotiated between the parties. Who owns the data under these agreements? Users, although not typically party to the contractual agreements, may see their rights and obligations affected by using cloud computing (i.e., where personal information is entered and stored, where users negligently give access to data to unauthorized third parties). How are third parties and third parties-related information affected by cloud computing agreements?

9. Fourth, the cloud service agreement can raise issues of conflict of laws. These conflicts can take place in relation to the various aspects of the contracts, which for different reasons are not subject to the same law. (For example, in some situations users are not party to the service agreements and are therefore not affected by a choice of law clause in the service agreement. In other situations, by application of public policy in various States, including consumer protection, privacy legislation and protection of confidential information legislation, different laws come into play.) These issues are likely to become increasingly prevalent, as well as more complex, in light of the fact that many cloud providers use multi-jurisdictional locations for their servers and operations.

10. Similarly, the interaction between choice of jurisdiction and jurisdictional rules on the one hand and public policy and connecting factors used to determine jurisdiction of a court on the other hand could lead to important challenges in practice. For example, would a choice of applicable law and jurisdiction between the service provider and the service applicant pointing to State A validly oust jurisdiction of the national courts in State B where a user is located? More generally, should the host be subject to disclosure requirements even though it has very limited connection to the jurisdiction ordering disclosure?

11. Fifth, what practical and effective measures to limit risks should be put in place by service providers? For example should service providers be encouraged to offer multi-tiered access with varying access privileges (i.e., not all personal information about an entity is accessible to all users)? Should they be required to inform potential clients of the availability or unavailability of such safeguards and multi-tiered access functions? Should they contract liability insurance and who should be responsible for insuring a particular risk? Is the cloud computing and related legal issues different in the government context versus in the business context and should different standards apply? Should the service provider be required to disclose that access to the data can be granted to a given State authority in the conduct of special investigative powers? Is the existence of legislation on the protection of personal information and compliance by the service provider with the legislation sufficient to exonerate the provider from liability?

IV. Work to be carried out by UNCITRAL

12. The Commission could request the Secretariat to gather information relating to cloud computing, and in particular to data hosting, software as a service (SaS), and other prevalent cloud computing solutions, and prepare a document outlining existing practices. Where appropriate the document could stress potential risks stemming from current practices in relation to conflict of laws, the lack of supporting legislative provisions in national laws giving effect to data hosting-related agreements, and the lack of harmonization of domestic laws. The work could be done in collaboration with The Hague Conference on Private International Law where issues of conflicts of laws are being considered. The document could outline where best practices are needed based on evidence of absence of legal recourses, perceived imbalance between the rights and obligations of cloud computing participants or other evidence. Finally, the document could point to work done by other organizations in relation to cloud computing, notably in relation to privacy and the protection of personal information, with the view of identifying gaps in the international trade law framework. The document could then be used by the Working Group to identify issues in need of practical legislative or other solutions and to discuss possible future work.