# Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction

FAYE FANGFEI WANG*

**Abstract**

As a result of technologic innovation and optimization, the advent of cloud computing may change the way we work, communicate with each other and share information. In the cloud-based environment, access to computing resources (such as storage, processing and software) has shifted from an internal network to a public network in particular in the public cloud environment. It may challenge the allocation of responsibility among cloud providers, cloud customers and cloud users. Subsequently it may affect the attribution of title to data controllers and data processors. This paper undertakes primary research and provides insights into the significant yet complicated determination of the validity of jurisdiction clauses for cloud service contracts and the intertwined issues regarding the balance between the cloud interoperability and the protection of data privacy and intellectual property rights. It addresses key legal challenges faced by cloud computing providers and users today and proposes possible solutions to establish greater legal certainty in cloud computing service contracts with reference to the current practice in the EU and US. In general, this paper argues that although the deployment of cloud computing may complicate the determination of jurisdiction when disputes arise, a well-negotiated and sophisticated service contract of cloud computing may minimise such risk.

## 1. Introduction

'Cloud Computing can be defined 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.'[1]

* Senior Lecturer in Law, Brunel Law School, Brunel University (UK). Email: faye.wang@brunel.ac.uk. The first section of the paper partly draws upon F Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (Cambridge: Cambridge University Press, 2010).

[1] The National Institute of Standards and Technology (NIST) Definition of Cloud Computing, U.S. Department of Commerce, Special Publication SP800-145, September 2011, available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed 1 February 2013), at 2.

In brief, it can be understood as, 'access to computing resources (storage, processing and software), on demand, via a network'.[2] This definition highlights the characteristics and benefits of cloud computing. That is, cloud computing is a cloud model of a computing design and global infrastructure that is available and accessible anywhere for remote storage and processing of data. This type of technologic innovation and optimization may change the way we work, communicate with each other and share information, because access to computing resources has shifted from an internal network to a public network in particular in the public cloud environment. There are also new participants in such new environment and as a result, it may challenge the allocation of responsibility among cloud providers, cloud customers and cloud users. Subsequently it may also affect the attribution of title to data controllers and data processors.

Despite the emerging challenges in the legal sphere, 'cloud wars' seem to be unavoidable – private entities such as Microsoft and Google have been competing over the winning of contracts for cloud computing services owing to the possible advantages of cost savings, speed improvement and mobile accessibility for governments, businesses and individuals. For example, the US Department of the Interior announced the selection of Google Apps over Microsoft for Government for Cloud Email and Collaboration Services on 1 May 2012 and this application is expected to save up to $500 million in taxpayer dollars by 2020.[3] The current statistical data also shows that the use of Internet and Networks (persons aged 16 to 74) has been continuously increasing worldwide,[4] which may also have an impact on the widespread use of cloud computing. The intended possible outcomes of cloud computing are to bring numerous benefits, and yet somehow, the deployment of such technology may involve higher risk, consume more energy[5] and cause legal complications.

In response to those challenges, governments have initiated or have been working on strategies of clouding computing for their states. For example, the US launched the Federal Cloud Computing Strategy on 8 February 2011, while it was anticipated that the European Commission would publish a strategy on stimulating cloud comput-

---

[2] Guidance on the Use of Cloud Computing, UK Information Commissioner's Office , 20121002 Version 1.1, October 2012, available at http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx (accessed 1 February 2013), at 1.

[3] Press Release 'Interior Selects Google Apps for Government for Cloud Email and Collaboration Services', The U.S. Department of the Interior, 1 May 2012, available at http://www.doi.gov/news/pressreleases/Interior-Selects-Google-Apps-for-Government-for-Cloud-Email-and-Collaboration-Services.cfm# (accessed 1 February 2013); See also Case no. 10-743, *Google, Inc. and Onix Networking Corporation v. The United States and Softchoice Corporation*, 4 January 2011, the United States Court of Federal Claims.

[4] *The EU in the World 2013: A Statistical Portrait* 82–83 (Eurostat European Commission, 2012) available at http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-30-12-861/EN/KS-30-12-861-EN.PDF (accessed 1 February 2013).

[5] G.Cook, *How Clean is Your Cloud?* (Greenpeace International, April 2012), available at http://www.greenpeace.org/international/Global/international/publications/climate/2012/iCoal/HowCleanisYourCloud.pdf (accessed 1 February 2013).

ing in Europe in 2012.[6] Developing an EU-wide strategy on 'cloud computing' notably for government and science was one of the eight action plans in the European Commission's Digital Agenda for Europe in 2010.[7] Subsequently, the Digital Agenda Annual Progress Report (hereinafter 'the 2011 Annual Progress Report') was issued on 22 December 2011. The 2011 Annual Progress Report has identified eight pillars of work on progress and emphasised that the purpose of launching an overall strategy on cloud computing is to provide 'a better offer of high-speed Internet and better communication infrastructure for more citizens'.[8] In 2011 there was also a public consultation on cloud computing in Europe conducted by the Commission. The public consultation was conducted between 16 May 2011 and 31 August 2011 and the Public Consultation Report on Cloud Computing (hereinafter 'the EU Public Consultation Report') was released on 5 December 2011.[9] However, the results of the public consultation on cloud computing in Europe were not mentioned in the 2011 Annual Progress Report. In order to benefit the employment of cloud computing in industries and daily life, not only a well-balanced country-level or region-level strategy on cloud computing is needed, but also the consistent application and implementation of such strategy that meets the international standards is required.

This paper undertakes primary research and provides insights into the significant yet complicated determination of the validity of jurisdiction clauses for cloud service contracts and the intertwined issues regarding the balance between the cloud interoperability and the protection of data privacy and intellectual property rights. It addresses key legal challenges faced by cloud computing providers, customers and users today and proposes possible solutions to establish greater legal certainty in cloud computing service contracts with reference to current practice in the EU and US. In general, this paper argues that although the deployment of cloud computing may complicate the determination of jurisdiction when disputes arise, a well-negotiated and sophisticated service contract of cloud computing may minimise such risk. The importance of this timely research can also be evidenced by the recent European Commission Decision of 18. 06. 2013 on setting up the Commission Expert Group on Cloud Computing Contracts (2013/C 174/04).

---

[6] Digital Agenda for Europe, *Annual Profess Report 2011* 3 (Brussels, 22 December 2011), available at http://ec.europa.eu/information_society/digital-agenda/documents/dae_annual_report_2011.pdf (accessed 1 February 2013).

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Agenda for Europe*, Brussels, 26.8.2010, COM(2010) 245 final/2, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF (accessed 1 February 2013), at 23–24.

[8] *Communication on E-Commerce – Frequently Asked Questions*, Reference: MEMO/12/5, 11/01/2012, Brussels, at 3.

[9] *Cloud Computing: Public Consultation Report* (European Commission, Brussels, 5 December 2011), available at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf (accessed 1 February 2013).

## 2. General Legal Complications of Cloud Computing

### *2.1. Legal Complications as to Different Models*

There are mainly four deployment models of could computing, namely private cloud, community cloud, public cloud and hybrid cloud. Hybrid cloud is a combination of private, community or public cloud. The cloud infrastructure of community, public and hybrid clouds is in common as it is open to different organisations, whereas private cloud is operated solely for one organisation.[10] In terms of service models, there are three main categories: (1) Cloud Software as a Service (SaaS) such as Google Docs; (2) Cloud Platform as a Service (PaaS) such as Facebook or Google App; and (3) Cloud Infrastructure as a Service (IaaS) such as Amazon.[11] SaaS is the simplest solution for accessing information or email anywhere as it provides end users applications, whereas PaaS is more suitable to be used to manage e-commerce processes as it provides customers the possibility to build and manage their own applications. IaaS allows customers to use their own operating systems and applications based on the cloud service provider's hardware and computing resources, such as storage and networks etc. Those three main service modules are to meet different business needs, requirements and functionalities, though layered services (the combination of those three main services) have also been rising so as to meet specific demands of business. Nevertheless, such combination often leads to a more complex supply chain of cloud providers[12] and the allocation of risk and responsibility among them.

### *2.2. Legal Complications as to the Definition of Parties*

In theory, by nature there are three main parties involving in the cloud-based environment: cloud providers, cloud customers and cloud users. By task allocation, there are also three main parties involving in the cloud-based environment: data processors, data controllers and end users.

Article 2 (d) of the EC Directive on Data Protection states:

> 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

---

[10] V. Kundra, *Federal Cloud Computing Strategy*, 5 (The White House, Washington, United States, 2011), 8 February 2011, available at http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf (accessed 1 February 2013).

[11] Kundra , *Federal Cloud Computing Strategy*, *op cit* at 6.

[12] See *Guidance on the Use of Cloud Computing,* 5 (UK).

Article 2(e) of the EC Directive on Data Protection provides:

> 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

According to the above definition, individuals or private entities (such as cloud providers, customers and users) involving in cloud computing is not easy to be defined as controllers or processors, because each individual or private entity might act in a double role, for instance, a 'cloud provider' could be acting as a 'data processor' and 'data controller' at the same time. The determination of the role of a cloud provider may depend on what work it involves by nature as showed in Figure 1 below:

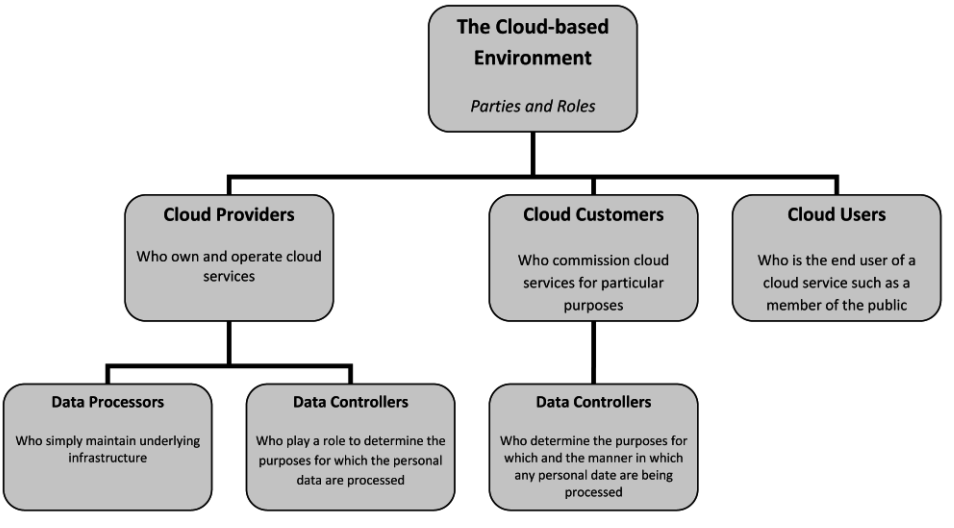


Figure 1. The Role of Parties in the Cloud-based Environments[13]

That is, if an organization that owns and operates a cloud service and simply maintains any underlying infrastructure, it is likely to be a 'data processor' which implements tasks such as 'allocating computing resources, performing and storing back-ups and providing support'.[14] If it plays a role in determining the purposes for which the personal data are processed (i.e., it uses the personal data for its own purposes), then it will also be a 'data controller'.[15]

It is important to determine whether the cloud provider is merely acting as a 'data processor' on behalf of the data controller or whether it is a 'data controller' in its

[13] See *Guidance on the Use of Cloud Computing,* 4–16 (UK).
[14] See *Guidance on the Use of Cloud Computing,* 8 (UK).
[15] See *Guidance on the Use of Cloud Computing,* 9 (UK).

own rights, because subsequently the legal responsibilities and liabilities will be different. Data controllers have primary responsibility for ensuring the safety, integrity and access of personal data. Therefore, data controllers have an overall responsibility complying with their national data protection rules.[16]

### *2.3. Legal Complications as to Balance*

It is notable that the use of cloud computing service also raises a wide range of legal concerns across almost every discipline and subject matter of law, no matter which type or category of cloud computing service model is chosen. In general, the threat to the use of cloud computing services mainly includes content infringement (e.g. data security, privacy and IP rights infringement) and performance infringement (e.g. non-compliance with the requirements of cloud computing services and/or product description). Those infringements may constitute criminal offences from a public law perspective. They may also constitute a breach of contract and/or be claimed for tortious liability from a private law perspective.

In the EU, the EU Public Consultation Report on Cloud Computing 2011 has summarised five key concerns on cloud computing, namely:[17]

1) The unclear rights and responsibilities of various parties in the cloud services;
2) The general lack of certainty in the legal framework, in particular regarding liability in cross-border situations;
3) The lack of guidelines and checklists on model terms for cloud computing services, for example, model Service Level Agreement (SLA) and model End User Agreement (EUA);
4) The diversity of Member State transpositions of the EC Data Protection Directive;
5) The need for future research to improve current cloud computing commercial offerings in terms of infrastructure.

The above concerns raise legal issues spreading across contract, torts, criminal law, jurisdiction, data protection and other relevant subject matters. The issue of data privacy protection has been particularly stressed, which is obviously at the heart of cloud computing regulation. However, jurisdiction and applicable law that are intertwined with other subject matters of law have not been explored.

In the US, the Federal Cloud Computing Strategy 2011 recognised the international dimensions of cloud computing and urged to consider issues such as:[18]

---

[16] EC Directive on Data Protection (1995), Recital (18), (19) and (32).

[17] See *Cloud Computing: Public Consultation Report* (European Commission, Brussels, 5 December 2011).

[18] Kundra, *Federal Cloud Computing Strategy*, *op cit* at 30.

1) Data sovereignty, data in motion, and data access: How do countries strike the proper balance between privacy, security and intellectual property of national data?
2) Are there needs for international cloud computing legal, regulatory, or government frameworks?
3) Cloud computing codes of conducts for national governments, industry, and non-governmental organisations;
4) Data interoperability and portability in domestic and international settings;
5) Ensuring global harmonisation of cloud computing standards.

As shown above, both the EU and US have flagged the need of international harmonization and standardization of cloud computing practice and legal protection. It is widely recognised that protection of users' rights in cloud-based services could be very challenging due to the characteristics of cloud computing and the constraint of bargaining power on the terms of contract between contracting parties. Customers and users may not be able to choose or restrict the location of data centres prior to the conclusion of the Service Level Agreement (SLA). Data centres may be relocated or added at any time and as a result they may be located in various jurisdictions which could contribute to the difficulty in identifying the location of infringement and determining the competent court and applicable law. This, leaving well alone other legal issues of cloud computing, furthers the existing challenges of Internet jurisdiction and choice of law for electronic commercial transactions which began in early 2000s.

One of the other possible contributing factors to the complexity of determining jurisdiction and applicable law may also be reflected on the need of striking proper balance between cloud interoperability, data interoperability and other rights protection. Both the EU and US seem to take the view that the public sectors should set the requirements for standards in data security, interoperability and portability. In addition, the public sectors should have relevant policy in place to encourage improvement in cloud infrastructure through research and innovation. The relationship between cloud interoperability and IP protection can be deemed to be one of the typical examples as this is an uneasy balance to strike from a social and economic point of view. That is, although 'cloud interoperability and data portability' increase efficiency and promote innovation, intellectual property (IP) rights may be used by the IP rights holders to prevent other cloud providers from interoperating the existing products. Such balance may be possible to be achieved through a sound legal infrastructure at community level, i.e. the interplay between the IP rights and competition rules which can be developed upon the previous experience of traditional software interoperability. This challenges the choice of competent court and governing law in terms of what exactly the subject and its scope is, and thus, a well-negotiated jurisdictional clause is of great essence to be included in the cloud computing service agreements.

## 3. The Validity of Jurisdictional Clauses in the Cloud-based Environment

### *3.1. The Benefits of Jurisdictional Clauses*

It is arguable that having international harmonised rules for cloud computing services will be a solution to balance potentially conflicting interests of both parties in different countries. However, regulatory decision-making takes time and its maturity also relies on the practical experiences from new industries. Meanwhile, recent legal experiences for the information society should be deployed by business and individuals to direct the booming industry and minimise the legal uncertainty.

It is inevitable that poor drafting contracts may affect the intended effects and expected outcomes. A sophisticated drafting of contractual terms of service for cloud computing is highly desirable as it may well increase the certainty and predictability of legal protection and yet avoid the complication of the determination of jurisdiction and applicable law as 'such clauses contribute to legal certainty in commercial relationships, since they enable the parties, in the event of a dispute, easily to determine which courts will have jurisdiction to deal with it'.[19]

In practice cloud service providers usually provide the standard Service Level Agreement (SLA) written for all their customers. SLA is a policy governing the use of cloud computing service between cloud service providers and their customers/users under the agreement of Cloud Provider Terms of Service. SLA usually defines the level of service such as the contracted delivery time of the service, performance or exclusion, whereas Terms of Service cover a wider range of issues such as rights and obligations, limitation of liability and governing law etc. For example, Google Terms of Service provides the Choice of Law and Court Clause (to be effective on 20 July 2012) as follows:[20]

16.10 *Governing Law*.

a. *For City, County, and State Government Entities*. If Customer is a city, county or state government entity, then the parties agree to remain silent regarding governing law and venue.
b. *For Federal Government Entities*. If Customer is a federal government entity then the following applies: This Agreement will be governed by and interpreted and enforced in accordance with the laws of the United States of America without reference to conflict of laws. Solely to the extent permitted by federal law: (i) the laws of the State of California (excluding California's choice of law rules) will apply in the absence of applicable federal law; and (ii) FOR ANY DISPUTE

---

[19] Case C-116/02, *Erich Gasser GmbH v. MISAT Srl*, Judgment of the Court (Full Court), 9 December 2003, para. 31.

[20] *Google App Engine Terms of Service*, Clause 16.20, available at https://developers.google.com/appengine/terms (accessed 1 February 2013).

ARISING OUT OF OR RELATING TO THIS Agreement, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

c. *For All Other Entities*. If Customer is any entity not set forth in Section 16.10(a) or (b) then the following applies: This Agreement is governed by California law, excluding that state's choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS Agreement, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

According to this clause, if customers (either business or consumers) use the Google App cloud computing service, California law will be the choice of law and the courts in Santa Clara County California will be the exclusive choice of courts when disputes arise. This is despite the possibility that '"Google may process and store an Application and Customer Content in the United States or any other country in which Google or its agents maintain facilities'.[21] The insertion of such choice of law and court clause in Terms of Service will avoid the complication of determining applicable law and jurisdiction as one of the connecting factors pertains to the location of data centers. If data centers of cloud computing service are located in the EU, in absence of a choice of law and court clause/agreement the determination of the competent court or applicable law should be subject to the country-of-origin principle under the EC Directive on Electronic Commerce (applicable law for both contractual and non-contractual matters)[22] alongside the Brussels I Regulation (jurisdiction for both contractual and non-contractual matters),[23] Rome I Regulation (applicable law for contractual matters)[24] and Room II Regulation (applicable law for non-contractual matters).[25] The great significance of the functions or benefits of the choice of law and court agreements has prompted speculation over the validity of electronic choice of law and court agreements in cloud computing service in particular when sub-contracts of sale or service may be automatically generated by electronic means in automated computing systems (i.e. under service-oriented computing modules). According to Figure 1, there is a possibility of having a sub-contract between cloud provider(s) and cloud customer(s)

---

[21] *Google App Engine Terms of Service*, Clause 2.2.

[22] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter 'EC Directive on electronic commerce'), Official Journal L 178, 17/07/2000 P. 0001–0016. Article 3(1) provides that 'Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field'.

[23] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16.1.2001, 1–23.

[24] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008, 6–16.

[25] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007, 40–49.

if they are different parties and/or sharing responsibility as data controller(s). If the jurisdictional clauses in the sub-contract were concluded after cloud users signed SLA and they are different from those of the SLA, they may have an impact on cloud users. In practice cloud users will not be informed about such information prior to the conclusion of sub-contracts between cloud providers and cloud customers. It may be worth considering a legal obligation to attain informed consent from cloud users regarding jurisdictional clauses of sub-contracts as this may affect cloud users' decision on the collection, storage, access and usage of personal data in the cloud-based environment.

In addition, the validity of choice of court agreements in cloud computing will be especially of concern because there is no uniformity at the international level. Currently, both the EU and US have signed but not ratified the Choice of Court Convention.[26] In the US, the Uniform Law Commission (ULC) has also been working on the implementation of the Choice of Court Convention and trying to resolve the remaining issues with regard to the enactment conformity between the state and federal courts. ULC proposed naming the instrument as 'Uniform Choice of Court Agreements Implementation Act in the US' in July 2011.[27] On 14 December 2010 the European Commission proposed reforms of the current legal framework for civil and commercial jurisdiction under the Brussels I Regulation[28] (hereafter "the Reform Proposal of the Brussels I Regulation"). One of the six proposed actions is to enhance the effectiveness of choice of court agreements which aims at bringing the harmonization with the Choice of Court Convention. The adoption of the Brussels I Regulation (recast) in 2012[29] is deemed to be a way forward to promote the ratification process of such international instrument in the EU or at the very least provide some legal certainty as to exclusive jurisdiction agreements for parties who are not domiciled in the EU.[30]

### *3.2. The Validity of Jurisdictional Clauses*

The issue of choice of court agreements is one of the most important aspects in the regime of international jurisdiction as an exclusive jurisdiction clause will give rise to legal certainty on the court which may hear the case and avoid prolonged paral-

---

[26] Convention on Choice of Court Agreements, concluded 30 June 2005, available at www.hcch.net/ index_en.php?act=conventions.text&cid=98 (accessed 1 February 2013).

[27] *Minutes of Meeting of the Executive Committee* (Uniform Law Commission, Vail, Colorado, 6 July 2011), available at http://www.uniformlaws.org/shared/docs/executive/ExecMin070611.pdf (accessed 1 February 2013).

[28] Proposal for a Regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast) 14.12.2010, COM (2010) 748 final, 2010/0383 (COD).

[29] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), hereafter 'Brussels I Regulation (Recast)', available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:EN:PDF (accessed 1 March 2013).

[30] Brussels I Regulation (Recast) 2012, Article 25.

lel proceedings in different countries. With the aim to 'promote international trade and investment through enhanced judicial co-operation,'[31] the Choice of Court Convention applies solely to 'international cases of exclusive choice of court agreements concluded in civil or commercial matters'.[32] The definition of 'exclusive choice of court agreements' was given by the Choice of Court Convention in Article 3, providing that 'a) exclusive choice of court means an agreement concluded by two or more parties that meets the requirements of paragraph c) and designates, for the purpose of deciding disputes which have arisen or may arise in connection with a particular legal relationship, the courts of one Contracting State or one or more specific courts of on Contracting State to the exclusion of the jurisdiction of any other courts; b) a choice of court agreement which designates the courts of one Contracting State or one or more specific courts of one Contracting State shall be deemed to be exclusive unless the parties have expressly provided otherwise.'

This definition contains five requirements: firstly, the agreement between two or more parties must exist; secondly, the form requirement must be satisfied; thirdly, the agreement must designate courts of one state, or one or more specific courts in one State excluding all other courts; fourthly, the designated court or courts must be in a Contracting State; and finally, the designated courts must be connected to a particular legal relationship.[33]

In the EU the Brussels I Regulation is in contrast to the Choice of Court Convention that the Brussels I Regulation not only applies to exclusive jurisdiction agreements but also non-exclusive jurisdiction agreements. The Brussels I Regulation supports exclusive choice of court agreements that '[I]f the parties, one or more of whom is domiciled in a Member State, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction. Such jurisdiction shall be exclusive unless the parties have agreed otherwise.'[34] The Reform Proposal further develops a harmonised conflict of law rule on the substantive validity of choice of court agreements by inserting some new wording in Article 23(1) that the chosen court shall have jurisdiction 'unless the agreement is null and void as to its substance under the law of that Member State' to be in line with the Choice of Court Convention. Some legal scholars have criticised the insertion of 'nullity' and 'voidness' principles as it may 'undermine the effectiveness of the choice of court agreements by re-opening the debates of separability and permissible role of national in determining the validity of choice of court agreements'.[35] The draft Report of the European Parliament in 2011 also suggested replac-

---

[31] Hague Convention on Choice of Court Agreements 2005, paragraph 1.

[32] Hague Convention on Choice of Court Agreements 2005, Article 1(1).

[33] Hartley & Dogauchi, *Explanatory Report on the 2005 Hague Choice of Court Agreements Convention* 38–39 (HCCH Publication, 2007), available at http://www.hcch.net/upload/expl37e.pdf (accessed 1 February 2013).

[34] Brussels I Regulation 2001, Article 23(1).

[35] A. Dickinson, *The Proposal for a Regulation of the European Parliament and of the Council on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters*

ing 'unless the agreement is null and void as to its substance' to 'provided that the agreement is valid as to its substance'.[36]

> In the author's view, the introduction of "null and void" for determining the validity of a choice of court agreement would enhance the effectiveness of exercising party autonomy on choice of court agreements and giving priority to the forum chosen by the parties. The introduction of the principle of "null and void" to the Brussels I Regulation is not intended to cause further complication of assessing the material validity of the parties' agreements as it should have been according to domestic law, but to produce harmonised standards between member states. Indeed, to maximise the positive effects and the efficient implementation of the "null and void" principle, the European Commission may need to give additional guidance and explanatory notes. One of the feasible solutions to enhance harmonised standards could be by illustrating standardised examples of valid exclusive choice of court agreements without rigidly restricting the validity to particular wording for such agreements.[37]

The Brussels I Regulation (Recast) finally incorporates the condition of 'null or void' under the Choice of Court Convention into its new rule of exclusive jurisdiction agreements. It provides that 'If the parties, regardless of their domicile, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction, unless the agreement is null and void as to its substantive validity under the law of that Member State. Such jurisdiction shall be exclusive unless the parties have agreed otherwise.'[38] This significantly improves the consistency in determination of a valid choice-of-court clause with the Choice of Court Convention.

In the US, choice of court agreements, known as 'forum selection clauses', have generally been upheld in courts unless they are unreasonable and unjust. For example, the case of *M/S Bremen v. Zapata Off-Shore Co.* indicated that forum selection clauses in commercial contract are prima facie valid and enforceable unless unreasonable.[39] It is clear that both of the EU and US jurisdictional rules validate the principle of party autonomy in choice of court agreements, but the material consent regarding the validity of such agreements still relies on domestic law. The chosen court will hear the case when national law recognises such agreement as valid. With the advent of infor-

---

*(Recast) ('Brussels I bis' Regulation)* 21 (European Parliament, September 2011; Sydney Law School Research Paper No. 11/58), available at http://ssrn.com/abstract=1930712 (accessed 1 February 2013).

[36] EP document 2010/0383 (COD) [28.6.2011], *Draft Report on the Reform Proposal for Brussels I Regulation* 17 (Committee on Legal Affairs, European Parliament).

[37] F. Wang, *Regulation of Internet Jurisdiction for B2B Commercial Transactions: EU and US Compared*, in P Jurčys, P. F. Kjaer and R. Yatsunami (ed.), *Regulatory Hybridization in the Transnational Sphere* 99–124, 111 (The Netherlands: Brill Publishing 2013).

[38] Brussels I Regulation (Recast) 2012, Article 25(1).

[39] *M/S Bremen v. Zapata Off-Shore Co.*, 407 U.S 1, 10 (1972).

mation technology, the interpretation of the validity of electronic choice of court agreements can be even more challenging.

Computing technologies make it possible to sell intangible/digitised goods or provide information service without the need of physical delivery. It provides small and medium-sized trading companies with lower market entry costs the possibility of extending geographic reach to a much larger market. This has undoubtedly improved economic efficiency, competitiveness and profitability, but also raises legal challenges to the determination of connecting factors for jurisdictional issues, such as the place of domicile, the place of business and the place of performance. The deployment of cloud computing further complicates an already difficult situation regarding Internet jurisdiction.

For example, a seller/provider ('X') is French and lives in London, but 'X' has an electronic trading company whose head office is in New York with its data centres that are located in Netherlands (Utrecht) and United States (California). A buyer/user ('Y') is Spanish and lives in Dublin, but 'Y' establishes his/her computing business in Germany. 'Y' entered into a contract with 'X' for Secure Account Trading Information Service to be provided online by an automated electronic system. Further decision-making regarding provision of services will be done automatically between these two frequent international trading companies with standard terms and conditions without any human interaction. Such automated systems design and offer a most favourable service package to the buyer based on the information that the buyer gives, history of choice preferences and other data sources that the seller collects such as market prices, currency exchange rates, new modules and other relevant elements. Once the supply matches the demand (it usually takes a few seconds), an international contract of service will be automatically concluded by the automated trading systems. Although business could benefit from such system in terms of convenience and efficiency, there is potentially legal uncertainty with regard to the validity of automated electronic agreements incorporating exclusive choice of court clauses.

Under these circumstances, if the system automatically chooses the Utrecht district court to hear their case when disputes arise, will this clause be valid and enforceable? If there is no choice of court clause that is selected, which court will be the competent court to hear the case?

In principle, using electronic means to incorporate a choice of court agreement into a contract has been generally recognised by international, regional and national legislation. The general scope of the Choice of Court Convention outlined in Article 1 reflects its applicability to the digital age, as the "international" feature of the Convention strongly supports global cross-bordered electronic transactions. In addition, recognition and application of choice of court clauses concluded electronically can be also found in another two articles of the Choice of Court Convention. Article 3(c) of the Convention expressly states that an exclusive choice of court agreement must be concluded or documented 'in writing; or by any other means of communication, which renders information accessible so as to be usable for subsequent reference.' The terminology 'by any other means of communication' should be deemed to include any electronic means. The wording of this provision is in line with Article 6(1) of the

UNCITRAL Model Law on Electronic Commerce 1996. Another provision of the Choice of Court Convention that implies the consideration of electronic communications is Article 13. Article 13 (1)(b) of the Convention provides that 'the party seeking recognition or applying for enforcement shall produce the exclusive choice of court agreement, a certified copy thereof, or other evidence of its existence'. The wording of 'or other evidence of its existence' implies the acceptance of evidential agreements concluded electronically.

In the EU, Article 23(2) of the Brussels I Regulation (or Article 25(2) of the Brussels I Regulation (Recast) 2012) also explicitly acknowledges agreements concluded by electronic means, stating that 'any communication by electronic means which provides a durable record of, the agreement shall be equivalent to writing'. It means that agreements exchanged over the network as a secured word document (i.e. a read-only document or document with entry password), or concluded by email and clicking an 'I agree' button may fall within the scope of Article 23(2) of the Brussels I Regulation. Such electronic exclusive jurisdiction agreements must be available to read, download and reprint. In addition, such agreement will also need to meet certain formal criteria of contractual agreements such as the mutual consent of the parties. The approval of parties' mutual consent will be complicated for an electronic contract automatically concluded by the automated computing system without any human interaction. Under such circumstances, evidence must be established to show that parties have agreed in writing to use an automated choice of court agreement concluded by the system itself; such practices have been established between parties themselves; or parties have been aware of such usage that is commonly accepted in international trade or commerce, especially in the particular trade or commerce concerned. This can be referred to Article 23(1) of the Brussels I Regulation (or Article 25(1) of the Brussels I Regulation (Recast) 2012) that an exclusive choice of court agreement conferring jurisdiction shall be either: '(a) in writing or evidenced in writing; or (b) in a form which accords with practices which the parties have established between themselves; or (c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned.'

It is arguable that a choice of court agreement incorporated into the click-wrap agreement will be valid. In the case of *Tilly Russ and Ernest Russ v. NV Haven- & Vervoerbedrijf Nova and NV Goeminne Hout* (known as "*Tilly Russ* case"), the ECJ held that a jurisdiction clause contained in the printed conditions on a bill of lading satisfies the conditions laid down by Article 17 of the Brussels Convention (now Article 23 of the Brussels I Regulation).[40] In the case of *Estasis Salotti di Colzani Aimo e Gianmario Colzani s.n.c. v. Rüwa Polstereimaschinen GmbH*, the court ruled that to meet the requirement of 'in writing or evidenced in writing', parties must sign the front of the contract inserting an express reference to general conditions that are

[40] Case 71/83 *Tilly Russ and Ernest Russ v. NV Haven- & Vervoerbedrijf Nova and NV Goeminne Hout*, Judgment of the Court of 19 June 1984.

on the back with a jurisdiction clause.[41] Such reference must be clear, have been communicated to other contracting parties and can be checked by a party exercising reasonable care.[42] With regard to an oral choice of court agreement, an oral agreement must be reduced to writing to satisfy the formal requirement. It would even be valid if the confirmation of that agreement was written only by one of the parties but was received by the other with no objection.[43]

With regard to meeting the criteria of established practices between parties or trade usages, the leading case *Mainschiffahrts-Genossenschaft eG (MSG) v. Les Gravières Rhénanes SARL* provides that 'under a contract concluded orally in international trade or commerce, an agreement conferring jurisdiction will be deemed to have been validly concluded under that provision by virtue of the fact that one party to the contract did not react to a commercial letter of confirmation sent to it by the other party to the contract or ***repeatedly paid invoices without objection*** where those documents contained a pre-printed reference to the courts having jurisdiction, provided that such conduct is ***consistent with a practice*** in force in the field of ***international trade or commerce*** in which the parties in question operate and the latter are **aware** or ought to have been aware of the practice in question.'[44] The *Mainschiffahrts-Genossenschaft eG (MSG)* case establishes the principle of 'consistency in practices' between parties and that it is for the national court to determine the awareness of a particular trade usage in international trade or commerce.

Compared with the EU, the US has a similar approach to the recognition of electronic choice of court agreements. In the case of The *ProCD, Inc. v. Zeidenberg*[45] case, it was held that the shrink-wrap agreements was valid and enforceable because the defendant Zeidenberg did read the terms and click acceptance to the licence which could be regarded as giving the consent to the terms. If Zeidenberg rejected the term, he would have returned the product. In the case of *Carnival Cruise Lines v. Shute*, it was held that a forum selection clause that was placed in small print in a travel contract was enforced.[46] This is identical to a forum selection clause incorporated into a click-wrap sale contract. Accordingly, click-wrap agreement should be valid and enforcement. The leading case of *Caspi v. The Microsoft Network*[47] further confirms that generally forum selection clauses concluded by clicking 'I Agree' or 'I Don't Agree' at any point while parties scrolling through the agreement are prima facie valid and enforceable but parties must be seen to have had adequate notice of the forum selection clause. The court further concludes that the issue of reasonable notice regarding a forum selection clause is a question of law for the court to determine.

---

[41] Case 24/76 *Estasis Salotti di Colzani Aimo e Gianmario Colzani s.n.c. v. Rüwa Polstereimaschinen GmbH* [1976] ECR 1931, para. 10.

[42] *Ibid*, para. 12–13.

[43] Case 221/84 *F. Berghoefer GmbH & Co. KG v. ASA SA* [1985] ECR 2417, paras. 15–16.

[44] Case C-106/95 *Mainschiffahrts-Genossenschaft eG (MSG) v. Les Gravières Rhénanes SARL*, Judgment of the Court (Sixth Chamber) of 20 February 1997, ECR 1997 Page I-00911.

[45] 86 F.3d 1447 (7th Cir. 1996).

[46] 499 U.S. 585, 111 S.Ct. 1522, 113 L.Ed.2d 622 (1991).

[47] 323 NJ Super. 118, 732 A.2d 528 (1999).

Having looked at the general possibilities regarding the recognition of electronic choice of court agreements in the EU and US, it can be asserted that the validity of an automated trading contract incorporating an exclusive choice of court agreement may be established to satisfy the formal requirement of jurisdictional rules in the EU and US, providing that (a) parties have the full awareness of such agreements; (b) such automated trading systems have been widely accepted in the industry; and (c) such practices have been widely known in the field of international trade or commerce in the digital age.

With the employment of cloud computing, when automated commercial transactions involve various places of performance and data are processed in different data centers, parties can restrict the location of data centers by agreeing upon certain data being stored and processed in certain data centers. However, this solution is only feasible when such service contract is constructed between business entities with more or less equal negotiation powers. Even if business entities achieve such limitation to data location, this may jeopardize the full advantages of using cloud computing infrastructure in organizations. It is possible that jurisdictional agreements can be automatically formulated according to a series of written codes/rules in automated computing systems. For example, the formula can be created as 'Each block of service within one contract of service should be restricted to one data center only and the location of such data centre should be at the closest place to the services provided. Parties should bring the lawsuits to the courts of the place where, under the contract, the services were provided or should have been provided.' No matter which methodology of formula is chosen, parties can also increase the predictability of the validity of automated jurisdiction agreements by inserting a statement in the main service contract of using automated trading systems such as 'The jurisdiction clauses that are automatically generated by automated trading systems should be valid and exclusive, provided that such choices are based on the recipient's indication of the place of performance in the systems.'Alternatively, it is also possible to establish the recognition of such trade customs in the field of automated trading systems by the endorsements of local, regional or state chambers of commerce. Although the validity of automated choice of court clauses is recognized in principle, the automated insertion of choice of court agreements for data protection in the cloud-based environment may provide less feasible protection for cloud users (when disputes concerning data breach occurs) than those for the sale of digital goods (when disputes concerning the delivery or quality of goods). It may be more predictable and protective to choose a selected list of courts for data protection in service-oriented computing in the cloud-based environments between cloud providers, cloud customers and cloud users upfront in the main service contract.

In the situation where there are complex automated transactions comprising a number of agreements, most of which contained non-exclusive jurisdiction clauses in favour of one court but one agreement contained an exclusive jurisdiction clause in favour of the other court, it is necessary for the court to ascertain the parties' intentions. The recent English case *UBS Securities LLC v. HSH Nordbank AG* concerning

jurisdiction clauses in complex financial transactions suggested that it was the dispute resolution clause 'at the commercial centre of the transaction'which intended to govern such disputes.[48] In this case, the exclusive English jurisdiction clause in the Dealer Confirmation only related to technical banking disputes but not to the heart of the transaction, whereas the non-exclusive New York jurisdiction clauses apply at the commercial centre of the transaction.

The effects of incorporating choice of court agreements may be various due to different jurisdictional rules on the material validity and proceedings. In the EU, the *Lis pendens* rule requires that where proceedings involving the same cause of action and between the same parties are brought in the courts of different Member States, any court other than the Court first seized shall of its own motion stay its proceedings until such time as the jurisdiction of the court first seized is established. It is arguable that the current legal framework of jurisdiction in the EU invites parallel proceedings due to the operational systems of the *Lis Pendens* Rule in Article 27 of the Brussels I Regulation, though the *Lis Pendens* Rule aims at preventing parallel proceedings where cases covering the same litigants and the same facts are brought in different Member States. In addition, the implementation of the *Lis Pendens* Rule may unavoidably result in prolonged proceedings. For example, the judgment of the famous case *Erich Gasser GmbH v. MISAT Srl*[49] interpreted the *Lis Pendens* Rule as 'meaning that a court second seised whose jurisdiction has been claimed under an agreement conferring jurisdiction must nevertheless stay proceedings until the court first seised has declared that it has no jurisdiction' and 'it cannot be derogated from where, in general, the duration of proceedings before the courts of the Contracting State in which the court first seised is established is excessively long' Such interpretation generates the unpredictability on whether a court chosen by parties has priority to decide on its jurisdiction and how long it takes for the court first seised to decline jurisdiction. Due to the procedural nature of the *Lis Pendens* Rule, parties may take advantage of such rule as a mechanism to frustrate or undermine a choice of court agreement, or delay a case brought to the designated court. This is known as 'torpedo'. It is of no surprise that the European Commission feels pressed to enhance the effectiveness of choice of court agreements in order to promote party autonomy, reduce risk of parallel proceedings, avoid conflicting legal outcomes and thus enhance legal certainty and fairness of jurisdiction.

Compared with the EU, jurisdictional rules in the United States *do not* generally include a *formal lis pendens* doctrine but courts may rely on the rule of *forum non conveniens* to decide on the dismissal of the case. That is, it is for the chosen court to determine whether a choice of court agreement precludes granting the *forum non conveniens* motion.[50] When the court concludes that an exclusive choice of court

---

[48] [2009] EWCA Civ 585.

[49] Case C-116/02, Judgment of the Court of 9 December 2003.

[50] WW Heiser, *The Hague Convention on Choice of Court Agreements: The Impact on Forum Non Conveniens, Transfer of Venue, Removal, and Recognition of Judgments in United States Courts* 31 University of Pennsylvania Journal of International Law 1013–1050, 1019 (2010).

agreement does not prevent granting the *forum non conveniens*, the designated/chosen court may be dismissed.[51]

At the international level, the Choice of Court Convention does not include a direct rule on *lis pendens*. So the court designated by the choice of court agreement may proceed notwithstanding parallel proceedings being brought elsewhere.[52] The Green Paper on the Review of the Brussels I Regulation in 2009 (hereafter 'the Green Paper') proposes several suggested solutions to enhance the effectiveness of choice of court agreements in the Community.[53] It includes the debate over maintaining or excluding the *lis pendens* rule, or introducing a standard choice of court clause. The Reform Proposal of the Brussels I Regulation by the European Commission in 2010 further clarifies its position including two amendments: '1) where the parties have designated a particular court or courts to resolve their dispute, the proposal gives priority to the chosen court to decide on its jurisdiction, regardless of whether it is first or second seised. Any other court has to stay proceedings until the chosen court has established or – in case the agreement in invalid – declined jurisdiction; … and 2) the proposal introduces a harmonised conflict of law rule on the substantive validity of choice of court agreements, thus ensuring a similar outcome on this matter whatever the court seised.'[54] Although the Reform Proposal has not excluded the *lid pendens* rule which would have been in line with the Choice of Court Convention, the insertion of the new provision as Article 29(2) introducing a six-month time limit for the court first seised to establish its jurisdiction would potentially strengthen the legal certainty and efficiency of jurisdiction agreements. Parties will not lose too much time for a wrong proceeding and so do courts seised the case. Moreover, the Green Paper suggested that the uncertainty surrounding the validity of the agreement could be addressed by prescribing a standard choice of court clause, which could at the same time expedite the decision on the jurisdiction question by the courts.

As a result, the Brussels I Regulation (Recast) provides for an exception to the general *lis pendens* rule. It states that

> in order to enhance the effectiveness of exclusive choice-of-court agreements and to avoid abusive litigation tactics, it is necessary to provide for an exception to the general *lis pendens* rule in order to deal satisfactorily with a particular situation in which concurrent proceedings may arise. This is the situation where a

---

[51] *Life of Am. Ins. Co. v. Baker-Lowe-Fox Ins. Mktg., Inc.*, 873 S.W. 2d 537, 540 (Ark. 1994).

[52] See note 37. *Life of Am. Ins. Co. v. Baker-Lowe-Fox Ins. Mktg., Inc.*, 873 S.W. 2d 537, 540 (Ark. 1994).

[53] *Green Paper on the Review of Council Regulation (EC) No 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters*, Brussels, 21.4. 2009, COM(2009) 175 final, Commission of the European Communities (hereinafter 'the Green Paper'), available at http://www.ipex.eu/ipex/cms/home/Documents/doc_COM20090175FIN (accessed 1 February 2013).

[54] Proposal for a Regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast) 14.12.2010, COM (2010) 748 final, 2010/0383 (COD), 9–10.

> court not designated in an exclusive choice-of-court agreement has been seised of proceedings and the esignated court is seised subsequently of proceedings involving the same cause of action and between the same parties. In such a case, the court first seised should be required to stay its proceedings as soon as the designated court has been seised and until such time as the latter court declares that it has no jurisdiction under the exclusive choice-of-court agreement. This is to ensure that, in such a situation, the designated court has priority to decide on the validity of the agreement and on the extent to which the agreement applies to the dispute pending before it. The designated court should be able to proceed irrespective of whether the non-designated court has already decided on the stay of proceedings. This exception should not cover situations where the parties have entered into conflicting exclusive choice-of-court agreements or where a court designated in an exclusive choice-of-court agreement has been seised first. In such cases, the general *lis pendens rule* of this Regulation should apply.[55]

Brussels I Regulation (Recast) also introduces 'the time that the court is deemed to be seised'.[56] However, the 'time limit' for the court first seised to decline jurisdiction has not been specified. The regulation of 'time limit' may be of great help in enhancing the effectiveness of exercising party autonomy on choice of court agreements and giving priority to the forum chosen by the parties. Nevertheless, the adoption of the Brussels I Regulation (Recast) has clarified various issues regarding the validity of jurisdictional clauses which also provides some helpful recognition for the validity of jurisdictional clauses concluded in the cloud-based environment.

## 4. Special Jurisdiction for Rights Infringement in Cloud-based Services

### *4.1. Data Privacy Protection*

Despite the benefits of using cloud computing for business, the core issue that concerns the users regarding cloud computing service must be the risk regarding data security and integrity. The Opinion 05/2012 on Cloud Computing from Working Group 29 adopted on 1 July 2012 specifies that 'businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis'.[57] It is suggested that 'the great use of cloud computing technologies also means that it will become increasingly difficult for individuals

---

[55] Brussels I Regulation (Recast) 2012, Recital (22); see also Article 29, 30 and 31.

[56] Brussels I Regulation (Recast) 2012, Article 32.

[57] Opinion 05/2012 on Cloud Computing (adopted on 1 July 2012), Article 29 Data Protection Working Party, 01037/12/EN, WP196, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (accessed 1 February 2013), at 2.

to exercise their rights with regard to data stored in other countries'.[58] Data breach can be sued for breach of contract or claimed for invasion of tort. As mentioned earlier the contract of cloud computing service can preclude data from being transferred among different jurisdictions by locating data centres restrictively in a single jurisdiction or selected jurisdictions in theory. In practice, it is subject to a number of constraints such as negotiation powers in particular between business and consumers. In absence of jurisdictional clauses, courts usually resort to national data protection law, private international law and other relevant national law for determining jurisdiction. In the cloud-based environment, often, data are not stored or processed in one particular data centre within the same country. The standard of data protection can be different between countries and yet business and individuals fear that data may not be adequately protected in a third country due to different standards in different countries. The differentiation between national legislation may affect the effective prevention of cross-border data security breach and the complexity of determining the competent court due to complicated connecting factors such as the establishment of the controllers (cloud customers/clients) and the location of data centres, which may pose a further threat to rights protection. In light of these alarming issues, regions or countries such as the EU and US have indicated the necessity of national-level action on the protection of international data transfers and its remedies (such as the jurisdiction provision) when breaches occur. While the US has taken the initiative to launch the federal cloud computing strategy, the EU has been reviewing its existing legal framework to adapt to challenges posed by the rapid development of new technologies.

In the EU, the EC e-Privacy Directive has been amended by the Directive 2009/136/EC[59] to keep in line with the current social and technological development, however the new EC e-Privacy Directive still leaves out the "applicable law and jurisdiction" provision. Meanwhile, EC Directive on Data Protection in 1995[60] has been under the review of European Commission since 2009. An official recommendation document called 'A comprehensive approach on personal data protection in the European Union' (known as 'the EU Comprehensive Approach 2010') was also issued on 4 November 2010 to address challenging legal matters for the communication from the Commis-

---

[58] C Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (OECD Digital Economy Papers, No.187, OECD Publishing 2011), available at http://www.oecd-ilibrary.org/docserver/download/fulltext/5kg0s2fk315f.pdf?expires=1342770125&id=id&accname=guest&checksum=67DE91399C070987A7EB0BBA92A7D616 (accessed 1 February 2013).

[59] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the European Union, L 337/11, 18 December 2009, P.0011 – 0036.

[60] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 008 , 12/01/2001 P. 0001 – 0022.

sion to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions.[61] During the consultation on the comprehensive approach, a large majority of shareholders raised the concern that 'the complexity of the rules on international transfers of personal data is considered as constituting a substantial impediment to their operations as they regularly need to transfer personal data from the EU to other parts of the world'.[62] It is suggested that there is a growing need to improve and streamline the current procedures for international data transfers. Recommended measures include examining the adequacy of data transfer procedures and specifying the criteria and requirements for the assessment of the level of data protection in a third country or an international organisation.

As a result from the consultation process, on 25 January 2012 the European Commission has proposed the General Data Protection Regulation, which contains provisions of 'Transfer of Personal Data to Third Countries or International Organisations' (Chapter V) and 'Remedies, Liability and Sanctions' (Chapter VIII). They intend to remove legal obstacles to cross-border data transfers and increase legal certainty to data security by ensuring the adequacy of the level of protection[63] (that is effectively and consistently the same level of protection[64]) when data are transferred to third countries. With regard to the issue of jurisdiction and applicable law, Article 3 of the Proposal of the General Data Protection Regulation – Territorial Scope – amends the current Article 4 of the EC Directive on Data Protection – National Law Applicable, which is arguably the 'applicable law' provision that intends to have an implication on the determination of jurisdiction. Other provisions that are related to the central rule of applicable law – Article 4 of the EC Directive on Data Protection – include Recital (20) and Article 17(3) of the EC Directive on Data Protection.

Furthermore, Article 75(2) of the Proposal of the General Data Protection Regulation provides a new rule on jurisdiction for data protection that 'Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers'. The Opinion 05/2012 on Cloud Computing from Working Group 29 also further clarifies the controller-processor relationship that is for cloud clients/customers as controllers and cloud providers as processors.[65]

---

[61] *A Comprehensive Approach on Personal Data Protection in the European Union,* Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM(2010) 609/3.

[62] Proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Commission, Brussels, 25.1.2012 COM (2012) 11 final, 2012/0011 (COD), at 4.

[63] See Proposal for a General Data Protection Regulation, European Commission 25.1.2012, Article 41.

[64] See Proposal for a General Data Protection Regulation, European Commission 25.1.2012, at 6.

[65] See *Opinion 05/2012 on Cloud Computing* (adopted on 1 July 2012), at 4–5.

The approach proposed in Article 75(2) of the Proposal of the General Data Protection Regulation can be deemed as the employment of the traditional concepts of 'general jurisdiction and special jurisdiction', which are similar to the rules under the Brussels I Regulation. For example, Article 2(1) of the Brussels I Regulation (or Article 4(1) of the Brussels I Regulation (Recast) 2012) provides the rule of general jurisdiction that 'Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State'. When data breach is sued for breach of contract, Article 5(1) of the Brussels I Regulation (or Article 7(1) of the Brussels I Regulation (Recast) 2012) shall apply, that is 'in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided'. When data breach is claimed for invasion of tort, Article 5(3) of the Brussels I Regulation (or Article 7(2) of the Brussels I Regulation (Recast) 2012) shall apply, that is 'in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur'. In addition, Article 5(5) of the Brussels I Regulation (or Article 7(5) of the Brussels I Regulation (Recast) 2012) provides the rule of special jurisdiction that 'as regards a dispute arising out of the operations of a branch, agency or other establishment, in the courts for the place in which the branch, agency or other establishment is situated.'

Moreover, Article 76(3) and (4) of the Proposal of the General Data Protection Regulation further specifies rules dealing with parallel proceedings which are regulated under the Brussels I Regulation. That is to say, Article 3, 75(2) and 76(3)(4) of the Proposal of the General Data Protection Regulation in conjunction with the Brussels I Regulation extend and advance the existing rule in Article 4, Article 17(3) and Recital (20) of the EC Directive on Data Protection. It is known that the EC Directive on Data Protection originally establishes two main grounds for determining jurisdiction of personal data processing. The original two main grounds from Article 4 of the EC Directive on Data Protection apply to the establishment of the controller that is (a) on the territory of the Member States and (b) from a third country (outside the EU) respectively. Where the establishment of the controller is within the member states, national law of that Member State will apply, and where the controller is not established on the Member State's territory, national law of a Member State may still apply on the conditions that (1) it was directed by public international law; or (2) it involves the use of equipment situated on the territory of the said Member State except for transit.

The first step in the development of the original grounds is that Article 75(2) of the Proposal of the General Data Protection Regulation furthers the scope of the establishment under the EC Directive on Data Protection from 'the controller' to 'the controller or processer'. It means that under the new proposal of the General Data Protection Regulation, not only the courts of Member State where the controller contracting the cloud computing services is established can hear the case, but also the courts of Member State in which cloud providers are located can hear the case. As discussed in Figure 1, data controllers can be either cloud providers or cloud customers, and sometimes both. Data processors usually refer to cloud providers. There is

need to clarify whether the courts of Member State should be deemed to be competent to hear the case if cloud providers stand solely as data processors but not data controllers. In other words, it raises concerns over the connection of the courts of Member State in which cloud providers are located, when cloud providers are not in the position to control the quality of data but process data only.

The second step in the development of the original grounds is that Article 3 of the Proposal of the General Data Protection Regulation changes the second part of the second ground, although it remains the first ground established in Article 4 of the EC Directive on Data Protection. The second part of the second ground – the use of equipment – has been modified to a more specific situation that is when the controller is not established in the Union, the Regulation (adopted by Member States) may still apply where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour. In other words, the Proposal of the General Data Protection Regulation makes it clearer that the mere physical location of data centres supporting cloud computing infrastructure may not immediately constitute the establishment of the territory for the determination of applicable law. The nature of data centres (certain purposeful activities such as offering and monitoring) will contribute to the determination of whether the controller or processor has an establishment in that territory where data centres are located. However, there is still need for further clarification and interpretation of the conditions – 'offering of goods and services' and 'monitoring of their behaviour'. It is suggested that 'offering of goods and services' should include free services provided without financial costs to the individual and 'monitoring of behaviour' should include tracking on the Internet but should not be tied to creating profiles as such.[66]

Although the provision of jurisdiction – Article 75(2) of the Proposal of the General Data Protection Regulation – introduces the principles of general and special jurisdiction to be in line with the Brussels I Regulation, it maintains the key connecting factor for the determination of jurisdiction – 'the establishment'. The interpretation of 'the establishment' for jurisdiction should be identical to that of applicable law within its Article 3. Recently the Working Group 29 raised the further concern that 'the possibility to bring proceedings before the courts in any Member State where the controller or processor has an establishment, regardless of whether this is the main establishment or the establishment where the relevant decisions on data processing are taken, can be problematic'.[67]

As discussed earlier, data breach may be subject to contractual liability and/or tortious liability. Depending on the nature of breach, they may be considered as civil matters and/or criminal matters. It has been debated on the connecting factors that constitute some kind of establishment for international jurisdiction regarding data

---

[66] *Opinion 01/2012 on the Data Protection Reform Proposals* (adopted on 23 March 2012), Article 29 Data Protection Working Party, 00530/12/EN, WP 191, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf (accessed 1 February 2013), at 9.

[67] See note 52, p 25. *Opinion 01/2012 on the Data Protection Reform Proposals* (adopted on 23 March 2012), Article 29 Data Protection Working Party, 00530/12/EN, WP 191.

protection: the place of establishment of the data controller, the place of storage or processing of personal data, place where the wrongful act occurs, residence of the data subject, the use of cookies or similar technologies in another State and the use of equipment.[68] Those assumptions stemmed from various legal instruments, such as the country of origin principle for both contractual and non-contractual matters from Article 3 of the EC Directive on Electronic Commerce;[69] the place of performance for B2B contracts from Article 5(1) of the Brussels I Regulation (or Article 7(1) of the Brussels I Regulation (Recast) 2012); the targeting/directing approach for B2C contracts from Article 15(1)(c) of the Brussels I Regulation (or Article 17(1)(c) of the Brussels I Regulation (Recast) 2012); and the effects approach (harmful effects) in matters relating to tort from Article 5(3) of the Brussels I Regulation (or Article 7(2) of the Brussels I Regulation (Recast) 2012). In the cloud-based environment, the location of data centres may constitute an establishment only when it meets different conditions of the determination of jurisdiction in different matters. For instance, if cloud providers and/or customers own several data centres in several Member States for B2B service contracts, the courts for the place of performance of the principal obligation have jurisdiction over the whole claim,[70] or the plaintiff could sue in the court for the place of delivery of its choice.[71] With regard to B2C service contracts, in order to determine whether cloud providers and/or cloud customers can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of the Brussels I Regulation, it should be ascertained whether, before the conclusion of any contract with the consumer (cloud user), cloud providers or customers were using that data center that are located in the said Member State to 'envisage doing business with consumers domiciled in one or more Member States'.[72] Factors that are capable of constituting evidence may include but not limited to 'the use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Mem-

---

[68] C Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)* 18 International Journal of Law and Information Technology 227 – 247, 236–239 (2010).

[69] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter 'Directive on Electronic Commerce'), OJ 2000 L 178, Article 3.

[70] Case 266/85 *Shenavai v. Kreischer* [1987] ECR 239.

[71] Case C-386/05 *Color Drack GmbH v. Lexx International Vertriebs GmbH*, [2007] I. L. Pr. 35, p 456.

[72] Joined cases C-585/08 and C-144/09 *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG* (C-585/08) and *Hotel Alpenhof GesmbH v. Oliver Heller* (C-144/09), Judgment of the Court (Grand Chamber) 07 December 2010, para.79.

ber States.'[73] Nevertheless, the very nature of sending, storing and processing data in multiple jurisdictions under the cloud computing infrastructure[74] causes the unavoidable complexity of the determination of jurisdiction. This urges a national-level action on implementing standardisation for cloud computing service contracts and establishing a well-balanced legal framework to stimulate economic growth and protect users' rights without jeopardising technological innovation and market development. Another most challenging balance to strike is between cloud/data interoperability and IP rights protection due to the complexity of intertwined subject matters.

### *4.2. Intellectual Property Protection*

Protection of IP rights in cloud-based services could be very challenging due to the characteristics of cloud computing. Data centres may be located in various jurisdictions which could contribute to the difficulty in identifying the location of IP infringement and determining the competent court and applicable law. For example, in the EU, while Article 2 of the Brussels I Regulations provides the general jurisdiction rule for IP rights infringement, Article 5(3) of the Brussels I Regulation (or Article 7(2) of the Brussels I Regulation (Recast) 2012) is a central clause governing the determination of special jurisdiction for IP rights infringement. According to the effects approach in Article 5(3) of the Brussels I Regulation (or Article 7(2) of the Brussels I Regulation (Recast) 2012), they may be multiple locations that can quality as the place where the harmful event occurs: (a) the place of the event giving rise to the damage; and (b) the place where the damage occurred.[75] It is most likely that parties may need to enforce their IP rights in courts of different countries.

Moreover, cloud providers may not always own IP rights in cloud operating system software. There is also concern about software piracy (illegally copying software programs) in particular to open source cloud computing software, which is built by communities of developers with publically available source codes that are potentially open to hackers and malicious users.

Access control will be of concern to the protection of cloud providers' IP rights. However, through license agreements, cloud service providers should be allowed to study, test and exploit functions in cloud operation system software because the employment of the functionality of a computer program will help achieving interoperability between the elements of various programs. In the recent case of *SAS Institute Inc. v. World Programming Ltd*, the Court of Justice of the European Union (ECJ) ruled that the functionality of a computer program and the programming language

---

[73] See Joined cases C-585/08 and C-144/09, para.93

[74] Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing,* available at http://www.priv.gc.ca/information/pub/cc_201003_e.cfm#ftn14 (accessed 1 February 2013).

[75] ThCJA van Engelen, *Jurisdiction and Applicable in Matters of Intellectual Property* 14 Electronic Journal of Comparative Law 6 (2010), available at http://www.ejcl.org/143/art143–19.pdf (accessed 1 February 2013).

cannot be protected by copyright.[76] This is to avoid the monopolization of ideas according to Directive 91/250/EEC that only protects the expression of a computer program such as the source code and the object code but not ideas and principles which underlie any element of a computer program.[77] That is, the expression of an idea will be protected, but not the idea itself. This ECJ ruling may have implications on the awaiting lawsuit of *Google v. Oracle* in the US that judges might be sceptical about Google violating Oracle's copyright by cloning Java application programming interfaces (APIs) for use in Android.[78] This means that there may be a possibility that the competitors of cloud service providers could produce similar functionality of cloud service programs.

Cloud service providers also have the responsibility of protecting cloud users' IP rights. The responsibility of cloud service providers for IP rights protection is a matter of great complexity as it is difficult to equalize the position for compliance conditions between cloud providers and other Internet service providers under the current EU legal framework. In principle, the general monitoring of the information transmitted and stored by Internet service providers is prohibited by the EC Directive on Electronic Commerce.[79] In the recent cases of *Scarlet Extended SA. v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[80] and *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*.[81], the ECJ ruled that Internet service providers (such as online social network providers) cannot be obliged to install a filtering system to prevent IP infringement, i.e. illegal downloads of files, unlawful use of musical and audio-visual work. This is to strike a fair balance between IP rights protection and the freedom to conduct business. However, the question is that how fair the balance can be for various Internet service providers. Should cloud computing service providers have the same level of obligation as other service providers such as online social networking services or online shopping forums? If not, to what extent should those cloud computing service providers be obligated? The EC Directive on Electronic Commerce provides exemptions from the rule of "no general obligation to monitor" in its Recitals (47) and (48). It was anticipated that cloud computing service providers were likely to rely more heavily on access controls

---

[76] Case C-406/10, *SAS Institute Inc. v. World Programming Ltd*, Court of Justice of the European Union, Judgement, Luxembourg, 2 May 2012.

[77] Council Directive of 14 May 1991 on the legal protection of computer programs (OJ 1991 L 122, p 42).

[78] Case No. 10-3561, *Oracle America, Inc v. Google Inc*, United States District Court, Northern District of California, Trial Begins: 16 April 2012.

[79] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ 2000 L 178, Article 15.

[80] Case C-70/10, *Scarlet Extended SA. v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Court of Justice of the European Union, Judgement, Luxembourg, 24 November 2011.

[81] Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV.*, Court of Justice of the European Union, Judgement, Luxembourg, 16 February 2012.

and technological protections in the cloud environment.[82] It is possibly reasonable to impose a higher level of technological protocols for the prevention of IP infringement in cloud computing as in the cloud environment it is difficult to detect the place where the harmful event occurred or may occur, or where the act of infringement is committed, which will be one of the key factors in determining jurisdiction and applicable law.[83] Thus, challenges of protecting IP rights in the cloud environment are mainly twofold: first is relating to the enforcement of IP rights as it is difficult to detect the location of the theft of using patented work or making unauthorised copies of copyright protected work in cloud computing services and thus contribute to the complexity of jurisdiction and applicable law; and second is regarding the responsibilities of cloud providers for IP rights protection as it is difficult to equalize the position for legal compliance between cloud providers and other Internet service providers under the current EU legal framework.

Although the recent ECJ judgments provided ruling in a software provision rather than a cloud context, the principle that the functionality of a computer program and the programming language cannot be protected by copyright can also be employed in the cloud environment to promote cloud interoperability. As to the matter of 'no general monitoring obligation', further consideration of compliance conditions should be given to cloud computing service providers, though general Internet service providers cannot be obliged to install a filtering system to prevent IP infringement to stick a fair balance between IP rights protection and the freedom to conduct business. From a macro perspective, a two-tier approach can be suggested to stimulating cloud interoperability, data portability and protecting IP rights in cloud-based services: one is through building a sound legal infrastructure at Community level and the other is through establishing guidance on legal compliance for cloud computing service contracts. Meanwhile, cloud computing platforms may develop their own jurisdictional rules for IP rights protection to attract and support developers in practice.

## 5. Conclusion and Recommendation

Cloud computing technology has been gradually adopted in industries. New innovative solution to such technology may continue emerging. The further complication to Internet jurisdiction by cloud computing is unavoidable due to the very nature of such technologies. As analysed above, the determination of jurisdiction for cloud computing is subject to a wide range of factors and legal instruments, for example, in the EU, courts may need to consider the application of the country-of-

---

[82] H. E. Gutiérrez, *Peering Through the Cloud: The Future of Intellectual Property and Computing* 20 The Federal Circuit Bar Journal 589 – 608, 604 (2010–2011).

[83] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 012 , 16/01/2001 P. 0001 – 0023, Article 5 (3); and Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31/07/2007 P. 0040–0049, Article 8(2).

origin principle under the EC Directive on Electronic Commerce (applicable law for both contractual and non-contractual matters), the interpretation of the 'establishment' of a controller or processor under the EC Directive on Data Protection (applicable law for both contractual and non-contractual matters) alongside the application of the general, special and exclusive jurisdiction rules under the Brussels I Regulation (jurisdiction for both contractual and non-contractual matters). It is suggested that the insertion of jurisdictional clauses in Terms of Service in cloud computing will reduce the legal uncertainty in ascertaining connecting factors in particular the location and function of data centers. In general, a sophisticated service contract of cloud computing may minimise risk of legal uncertainty in dealing with cloud computing services.

Harmonisation of international jurisdictional rules for cloud computing services may also be a way forward to balance potentially conflicting interests of both parties in different countries. However, the process takes a long time and its maturity also relies on the experiences from new industries. This urges a national-level action on implementing standardisation for cloud computing service contracts based on previous experiences in e-commerce and meanwhile, working on the establishment of a well-balanced legal framework at the international level. In the author's view, the prioritized action plans should include:

1) To stimulate economic growth and protect users' rights without jeopardising technological innovation and market development;
2) To strike the balance between 'cloud/data interoperability' and 'IP rights and data privacy protection';
3) To standardise service contracts of cloud computing taking into account parties' different negotiation powers;
4) To continue modernising private international law in particular international jurisdiction in cloud computing.

The above listed action points fall within and expand the horizons of the current common working or proposed strategy in countries – the US has been the pioneer of putting the Federal Cloud Computing Strategy into action, while the EU has made steady progress on its work towards an EU-wide strategy for cloud computing. Undoubtedly the pilot regulatory framework of cloud computing in the US and EU will be of significant to the healthy growth of the new economy around the globe in the coming years.