

Jurisdictional Aspects of Cloud Computing

Prepared by
Cristos Velasco San Martin*
February 28, 2009

This essay discusses the problematic that “*cloud computing*” brings to the legal field, particularly the challenge of finding the most appropriate jurisdiction and forum for a country or state to launch a criminal investigation and prosecute an offender under international law.

Likewise, this essay analyzes the scope of the current definitions on cloud computing, provide examples of existing models, but most important, it will discuss the main legal aspects and challenges that this ubiquitous and novel concept brings to the current legal field. To this end, we will specifically analyze whether the provisions on jurisdiction of the Council of Europe’s Convention on Cybercrime could and should be applied when, for example, an illicit access, hacking or modification of software and systems occurs in the “*cloud*” or in case of a misuse of a device that leads to the perpetration of a crime in cyberspace having repercussions in multiple jurisdictions, and to what extent are countries legitimized to prosecute it.

Finally, it will be assessed whether there is a need to create future policy developments in the international arena in order to provide for better legal certainty in the field of cybercrime law.

1. Definition

With the advent of Web 2.0, the use and dissemination of blogs, wikis, it is now very common to hear the term “*cloud computing*”. But what exactly is involved every time this term is used. Pew Internet, a US think tank working on social aspects of the internet defines ‘*cloud computing*’ as follows: “*an emerging architecture by which data and applications reside in cyberspace, allowing users to access them through any web-connected device*”.¹

Under our own conception, “*cloud computing*” is the migration or outsourcing of computing, hardware and storage functions to a third-party service provider, which host applications on cyberspace through linked servers located worldwide. The term is often used in the same context as *grid computing* or *utility computing*.² The word “*cloud*” and

* Director General of the North American Consumer Project on Electronic Commerce (NACPEC) <http://www.nacpec.org/en/> and Ciberdelincuencia.org <http://www.ciberdelincuencia.org/info/acerca.php>

¹ John B. Horrigan, “*Use of Cloud Computing Applications and Services*”, Data Memo, Pew Internet & American Life Project, p.1., September 2008, available at: http://pewinternet.org/pdfs/PIP_Cloud.Memo.pdf (Last visited: February 28, 2009).

² See the definition of “*Grid computing*” in Wikipedia at: http://en.wikipedia.org/wiki/Grid_computing (Last visited: February 28, 2009).

“cyberspace”³ are often used not only as synonyms, but especially like metaphors in order to describe the use of applications and online activities based somewhere in the web.⁴

In a recent paper published by the University of California at Berkeley, the authors define cloud computing as: “*the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services*”. That paper mentions that such services have been long referred to as “*Software as a Service (SaaS)*”, and that the datacenter hardware and software is usually what is called a “*Cloud*”. The paper makes the distinction between “*Public Cloud*” and “*Private Cloud*”. Public Cloud is when a cloud is made available to the general public on a paid basis, and the service being sold is known as “*Utility Computing*”. While the term Private Cloud “*refers to internal datacenters of a business or other organization, not made available to the general public*”. Thus, according to the authors, cloud computing “*is the sum of SaaS and Utility Computing, but does not include Private Clouds, and people can be users or providers of SaaS, or users or providers of Utility Computing*”.⁵

2. Examples of Cloud Computing Models

The widespread development of ICTs, broad-band penetration, the explosion and growth of Web 2.0 applications, the proliferation of personal hand held devices with access to the internet, and the availability of wireless networks, each have played an important role in creating the cloud computing model. Cloud computing is a business model that provides numerous advantages to large and medium technology companies because they do not have to invest in new infrastructure, handle and manage computer systems and servers, provide security measures and back ups, train staff or license new software. In other words, all the said activities are outsourced to other companies or third party service providers, which handle the tasks and work for them.

For internet users and technology consumers, *cloud computing* means any online activity, which can be done from different devices; for instance, the use of e-mail services such as Yahoo and Gmail; storage of photos through websites like flickr or picasa; storage of videos through video online channels like Youtube; use of software programs and social networks such as myspace and facebook; word processing and storage of computer files based on the internet through Google Apps. The said activities are among the most popular cloud computing activities among users, and they are having a tremendous impact in our life and the way we communicate.

³ The term cyberspace has been around since the early eighties when William Gibson first coined it in his novels “*Burning Chrome*” and “*Neuromancer*”, while *cloud computing* is a concept that has been used only very recently, particularly with the advent of the Web 2.0.

⁴ See InfoWorld, “*What cloud computing really means*”, April 7, 2008, available at http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality_1.html (Last visited: February 28, 2009).

⁵ Michael Armbrust, Armando Fox, et al. “*Above the Clouds: A Berkeley View of Cloud Computing*” Electrical Engineering and Computer Sciences University of California at Berkeley, p.4., February 10, 2009, available at <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf> Last visited: February 28, 2009).

3. The Main Legal Aspects

As mentioned in previous lines, cloud computing offers numerous advantages to the end user, but it also gives rise to many legal and policy implications, which have not been fully addressed like privacy and data protection issues⁶, intellectual property rights, conflicts of laws, and applicable law and jurisdiction in the field of cybercrime. For purposes of this essay, we will only touch on aspects of privacy & data protection and more specifically with regards to the aspect of cybercrime jurisdiction.

3.1. Privacy and Data Protection Aspects

Perhaps, one of the main concerns that cloud computing raises today is data protection issues, mainly because the user's data are not stored in his own computer, but rather is accessed through the internet at a remote location from any device such as a laptop, mobile phone, or personal digital agenda. Furthermore, there is also the general concern that companies may use such data for purposes not originally specified, and to offer targeting advertising to the user.⁷ Pew Internet's survey on the use of cloud computing services reports high levels of concern among user when presented with scenarios in which companies may put their data to uses of which they may not be aware. Pew Internet provides the following statistics: "90% of cloud application users say they would be very concerned if the company at which their data were stored sold it to another party. 80% say they would be very concerned if companies used their photos or other data in marketing campaigns, and 68% of users say they would be very concerned if companies who provided cloud computing services analyzed their information and then displayed ads to them based on their actions".⁸

Another relevant concern in this area is that the user is not longer in control of his personal information, an aspect that breaks the whole concept of *informational self-determination*⁹, which is one of the international accepted privacy principles, and forms the basis of data protection laws worldwide.¹⁰ Other relevant questions that the cloud computing trend raises are: (i) who owns and controls data in the cloud?; (ii) is it or should it be a shared responsibility between companies and third party service providers?; and (iii) who should be accountable/liable in case of misuse? According to the Office of the Information Privacy Commissioner of Ontario what is needed in order to provide certainty to consumers and minimizing the risk of identity theft and fraud is a flexible and user centric identity

⁶ See Anne Cavoukian, "Privacy in the Clouds. A White Paper on Privacy and Digital Identity: Implications for the Internet", p.7., available at <http://www.ipc.on.ca/images/Resources/privacyinthecLOUDS.pdf> (Last visited: February 28, 2009).

⁷ Pew Internet, *supra* note 1, p.6.

⁸ Pew Internet, *supra* note 1, p.2.

⁹ Informational self-determination is defined by the Office of the Information Privacy Commissioner of Ontario as "the ability of individuals to exercise personal control over the collection, use and disclosure of their personal information by others". See Anne Cavoukian, *supra* note 6, p.2.

¹⁰ See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html (Last visited: February 28, 2009).

management system¹¹ where users can have control over their personal information and how it is used.¹²

Another relevant issue is the question of cross-border data flows and the location of the cloud provider. So for example, how could a company know when data is transferred outside “the cloud” and out of its territory? What happens if the data is transferred outside Europe –a continent with strong privacy and data protection laws¹³- to a country where no data protection laws are so far available like for instance Mexico or Guatemala? How could the exact location of the cloud provider be determined? What remedies and legal instances are available to the user? These and other questions are currently at the centre of the privacy debate, and they are the subjects of analysis in recently published papers.¹⁴

3.2. Jurisdictional Aspects

The concept or definition of jurisdiction varies from one country to another, and its scope relies very much upon the tradition of a legal system and its approach by the local courts and tribunals.¹⁵ However, when we talk about jurisdiction, we normally refer to include two main legal aspects: (i) to what extent a court or tribunal is legally competent to know about a dispute, and apply the jurisdictional rules of the place where the parties are located; and (ii) when a court or tribunal is entitled to assert jurisdiction as a result of a dispute arising between two parties or as result of illegal activity.

Perhaps, one of the greatest legal challenges that cloud computing creates is precisely the question on how to resolve jurisdictional issues and application of national criminal legislation as a result of illegal and wrongful conduct online, the conduct of which may have effects in one or multiple places. What happens if a perpetrator has illegal access to financial information of a national of Brazil who may happen to have bank accounts in the US and Switzerland and that have both been compromised by other hackers based in Ukraine? What laws should apply and which authorities and courts are legitimized to launch an investigation, prosecute the crime and the perpetrators?

As a result of globalization, the free movement of individuals and the wide spread in the use of ICTs, there are a wide number of case scenarios on the intersection between cyberrime jurisdiction and the ubiquity of cloud computing services that raise confronting

¹¹ Identity management systems offer the possibility of reducing the use of multiple user names and password for each online service, while maintaining privacy and confidentiality of personal information.

¹² Anne Cavoukian, *supra* note 6, p. 10.

¹³ See Europe’ legal framework on privacy and data protection at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#directive (Last visited: February 28, 2009).

¹⁴ See for e.g. Robert Gellman. “Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing” February 23, 2009, World Privacy Forum, available at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (Last visited: February 28, 2009).

¹⁵ See Cristos Velasco, “A Propósito de la Jurisdicción y el Derecho Aplicable en Internet”, Entérate en Línea, Dirección General de Servicios de Cómputo Académico de la Universidad Nacional Autónoma de México (DGSCA-UNAM, November, 2005), available at <http://nacpec.org/docs/CristosVelascoJurisdiccion.pdf> (Last visited: February 28, 2009).

legal and policy issues. Cloud computing has just started to deserve the attention of the private sector and national governments of developing nations.¹⁶

Unfortunately, not all countries are keeping pace with the development of policies regarding the *cloud computing* trend since most of them have not legislation in place against computer systems attacks and internet related crime.¹⁷

The enforcement aspect is another difficult issue to resolve, not only due to the difficulty of tracing perpetrators but also because they are often physically located in jurisdictions with weak, or without computer and internet criminal laws, making their prosecution very challenging for law enforcement authorities.

In the following section, we will analyze whether the *Council of Europe Convention on Cybercrime (hereinafter CoECC)*, specifically Article 22 on jurisdiction could apply to cloud computing scenarios.

3.3. Jurisdiction under the Convention on Cybercrime

The question of resolving jurisdictional aspects to information technology crimes has been an ongoing issue of debate in international organizations but particularly within the Council of Europe¹⁸, which is the organization promoting access to and ratification of the *CoECC* among European Member States and non-European States since 2001.¹⁹

Article 22 of the *CoECC* specifies the criteria under which contracting states are obliged to assert jurisdiction over criminal offenses provided in Articles 2-11 of the Convention.²⁰ We are of the opinion that the great majority of offenses committed under the cloud computing trend might likely fall under the first two categories of the Convention on Cybercrime “*Offenses against the confidentiality, integrity and availability of computer data and systems (Articles 2-6)*” and “*Computer-related offenses (Articles 7-8)*”. Under

¹⁶ See Krishnan Subramanian “*Barack Obama and Cloud Computing*”, November 5, 2008, available at: <http://www.cloudave.com/link/barack-obama-and-cloud-computing> (Last visited: February 28, 2009).

¹⁷ For instance, in Latin America, only four countries have enacted legislation against computer attacks and internet related offenses. Other countries have spread out provisions at the federal and state levels, and others rely on existent substantial and procedural provisions provided in their national codes.

¹⁸ The website of the Council of Europe is available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp (Last visited: February 28, 2009).

¹⁹ The Convention on Cybercrime is the only international treaty dealing with computer systems and internet-related offenses. It was officially opened for signature in Budapest on 23 November 2001, and it has been ratified by 22 countries and signed but not yet ratified by 21 others. The text of the Convention and its ratification chart is available at: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG> (Last visited: February 28, 2009).

²⁰ Such criminal offenses are divided into four major categories. Under the first category “*Offenses against the confidentiality, integrity and availability of computer data and systems*” are: (i) illegal access; (ii) illegal interception; (iii) data interference; (iv) system interference; and (v) misuse of devices. The second category “*Computer-related offenses*” are: (i) computer-related forgery; and (ii) computer related fraud. The third category “*Content related offenses*” are (i) offenses related to child pornography. And the fourth and last category deals with “*Offenses related to infringements of copyright and related rights*”.

such categories, contracting states may establish jurisdiction over criminal offenses like data espionage, hacking, identity theft and financial fraud.

The ubiquity of cloud computing, the borderless nature of the internet and the principles that govern the exercise of criminal jurisdiction completely challenges the legal system of a state in order for its local courts to be able to apply their national laws and launch a criminal investigation. This is mainly because the place where a crime occurs (*locus delicti*) could not precisely be determined under cloud computing. The first possible idea that might likely come to the mind of a Judge or Magistrate in order to assert jurisdiction over an offense occurring in cyberspace is to prosecute it pursuant to the location of equipment, server, database, software, or website. But how could a Judge, Magistrate with a typical legal formation and with no additional technical skills and knowledge, be able to approach the issue under this hypothesis? And what if the country where the Judge resides does not have substantive and procedural criminal legislation against attacks to computer systems and the internet? Another important question that deserves attention is what if more than one country has jurisdiction over a criminal offense, which of them will have priority to launch an investigation and under which legal foundations?

3.4. Application of Article 22 of the Convention on Cybercrime

The main purpose of Article 22 of the *CoECC* is that the contracting parties establish a required level of extraterritorial jurisdiction in relation to information technology offenses by determining three relevant aspects: (i) the place where the offense was committed; (ii) which laws should accordingly apply in case of multiple jurisdictions; and (iii) how to solve positive and how to avoid negative jurisdiction conflicts.²¹

Paragraph 1, section (a) of Article 22 allows a Party to prosecute a crime when it happens within its national territory. The Explanatory Report provides guidelines on this regard: “*a Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory even if the attacker is not*”.²² Paragraph I, section (b) and (c) requires each Party to establish criminal jurisdiction over offenses committed on board a ship flying the flag or aircraft registered under the laws of that Party, an obligation widely accepted under public international law, and provided in the laws of most States.²³

Paragraph 1, section (d) requires each Party to establish jurisdiction when the offense is committed by one of its nationals, if the offence is punishable under criminal law where it was committed, and if the offense is committed outside the territorial jurisdiction of any State. According to the Explanatory Report, the nationality principle is a theory most

²¹ Henrik W. K. Kaspersen, “*Jurisdiction in the Cybercrime Convention*” in “*Cybercrime and Jurisdiction. A Global Survey*” (Ed. Bert-Jaap Koops & Susan Brenner), Chapter Two, p.10., Information Technology & Law Series 11, 2006 T.M.C. Asser Press, The Hague.

²² See Council of Europe Explanatory Report of the Convention on Cybercrime (ETS No. 185), paragraph 233, available at: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> (Last visited: February 28, 2009).

²³ See e.g. Article 12 and 13 of Mexico’s Federal Civil Code.

frequently applied by countries with a civil law system, and under this section, Parties have the ability to prosecute a national even if he commits an offense abroad.²⁴

Paragraph 2 allows the parties to make reservations only in specific cases regarding sections (b), (c) and (d) of Paragraph 1. However, no reservation is permitted with regards to the establishment of territorial jurisdiction under section (a) or as the Explanatory Report mentions: “*in cases falling under the principle of “aut dedere aut judicare (extradite or prosecute)”*”, where for example, a country refuses to extradite an alleged offender on the basis of his nationality and the offender is present on its territory.²⁵

Paragraph 3 requires each Party to adopt the necessary measures to establish jurisdiction over extraditable offenses referred to in Article 24 paragraph 1 of the Convention. The Explanatory Report provides that jurisdiction under this paragraph “*is necessary to ensure that those Parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if sought by the Party that requested the extradition*”.²⁶

Paragraph 4 stipulates that the Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. This paragraph allows the Parties to establish other types of criminal jurisdiction in conformity with their national law.

Paragraph 5 provides a consultation mechanism for the Parties when more than one claims jurisdiction over an alleged offense established in accordance with the Convention. To this end, the Parties involved shall consult with a view to determine the most appropriate venue for prosecution of criminal activity without affecting the sovereignty of their own country. This paragraph is particularly useful as there will be occasions in which more than one Party has jurisdiction over some or all of the participants in crimes committed using computer systems and the internet. Under this provision, one of the Parties may be able to prosecute the main crime perpetrator while the others could deal with other possible participants of the crime, as in the case of organized crime.²⁷

Further, it should be noted that EU Members States have additional rules with regard to the assertion of jurisdiction over attacks against information systems provided in the Council Framework Decision 2005/222/JHA of 24 February 2005.²⁸

²⁴ *Supra* note 22, paragraph 236.

²⁵ *Ibid*, paragraph 237.

²⁶ *Ibid*, paragraph 238.

²⁷ See Henrik W. K. Kaspersen, *supra* note 21, p.18.

²⁸ The purpose of that Decision is to improve cooperation between judicial and other competent authorities, including the police and other specialized law enforcement services of European Member States, through approximating rules on criminal law in the area of attacks against information systems, and to contribute to the fight against organized crime and terrorism. The Council Framework Decision 2005/222/JHA of 24 February 2005 is available at:

http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf Last visited: February 28, 2009).

Article 10 of such Decision allows Member States to establish jurisdiction over the following offenses: (i) illegal access to information systems; (ii) illegal system interference, (iii) illegal data interference and; (iv) instigation, aiding and abetting and attempt, where the offense has been committed:

(a) in whole or in part within its territory, or

(b) by one of its nationals; or

(c) for the benefit of the legal person that has its head office in the territory of that Member State.

European Member States, by and large, have a solid legal framework and mechanisms in place for the prosecution of computer related crime, which are provided at the level of a treaty and a recommendation in order to ensure effective police and judicial cooperation against criminal offenses related to attacks against information systems. However, legal obstacles remain, when the perpetrator is not a national of the EU; when the offense was committed outside Europe; and even more when the State where the crime was committed is not a party to the *CoECC*.

Final Considerations

Cloud computing has challenging implications to the legal field, and therefore, effective policies are needed at the international and national levels in order to provide legal certainty to cloud computing services and their users. Such policies shall clearly establish how the enforcement of data protection laws should be applied in order to safeguard and protect the confidentiality and personal information of users, particularly with regards to the issue of cross-border transfers of data.

Cloud computing has also significant implications to the criminal law field, especially when it comes to the enforcement of legislation against a perpetrator based in another jurisdiction. It is important to point out that when a country establishes jurisdiction over a criminal offense committed over computer systems or through the internet, it does not mean that the state is bound to investigate it and prosecute the offenders. Many aspects play an important role in order for a State to determine jurisdiction and the prosecution of a cybercrime; for example internal domestic criminal policies, availability of financial and human resources, timeframe for investigation and execution and the country's political agenda.

Article 22 of the *CoECC* represents the consensus of traditional accepted principles of jurisdiction under public international law. However, the question of jurisdiction and cloud computing involves other issues such as transborder investigations of computer data, search and seizure of equipment and files, the determination of the place where the crime was conducted, the location of the criminal at the time of the attack, and the place or places where the damage and harm was felt. All these issues are partially considered under the scope of the *CoECC*. Therefore, the Council of Europe should create future policies, and perhaps the prospect of drafting an additional protocol, establishing guidelines and possible solutions on the intersection between cloud computing and cybercrime jurisdiction. The creation of such policies will have to revisit the jurisdictional approaches on cybercrime between common law and civil law countries, their practical approaches including tribunal

decisions and jurisprudence in this area, and should also emphasize the need to uniform frameworks, investigation, and law enforcement powers between states.

Finally, it should be pointed out, that substantial, as well as procedural cybercrime legislation, are essential elements for the investigation and prosecution of criminal offenses committed over computer systems and mobile devices. Without them, countries will not be able to coordinate their legal responses and cooperate in the global fight against cybercrime.