Harnessing the Cloud: International Law Implications of Cloud-Computing

Vineeth Narayanan
Harnessing the Cloud: 
International Law Implications of Cloud-Computing 
Vineeth Narayanan*

Abstract

For decades, with the advent of better and faster computer chips, processor speed has grown exponentially, and with it, the demand for computing power. Now, as that growth slows due to technological bottlenecks, the world will look to solutions like cloud-computing to ensure that the ever-increasing demand of computing power is met. Thus, the need for efficient, reliable, and powerful cloud-computing services will lead to and necessitate global cloud-computing service providers. But their vitalness will also bring cloud-computing under the scrutiny of government regulation, as countries struggle to ensure that the data of their citizenry is protected. This Comment explores the intersection of cloud-computing and international law by examining two states of the world, one in which countries attempt to give their data protection laws extraterritorial effect and the second in which countries organize to provide a global solution to the regulation of the cloud. The Comment finds that though there is justification under existing international law for countries’ cloud computing regulations to have extraterritorial effect, cooperation will yield greater adaptability for the regulatory system and stability for the computing cloud itself.

Table of Contents

I. Introduction ....................................................... 784
II. Cloud-Computing ........................................ 785
III. International Law Jurisdiction for Cloud-Computing Regulation .......... 789
   A. Preliminary Assumptions........................................ 789

* JD 2011, The University of Chicago Law School. The author would like to thank Shawn Liu, Milan Brahmbhatt, Davashish Awasthi, and Timothy Greene for their helpful comments and suggestions. The author would also like to thank the staff and board of CJIIL for their prudent and judicious editing.
I. INTRODUCTION

In 1961, John McCarthy, the man who coined the phrase “artificial intelligence,” predicted computing power would become a public utility, that is, a service directly provided or heavily regulated by the government.1 Today, personal computers have become ubiquitous, and cloud-computing, which provides shared public access to a modern necessity, is subject to increasing regulation, coming close to fulfilling McCarthy’s prediction. As more and more data, applications, and even entire operating systems are uploaded to the cloud, a public utility of another form is emerging: a global cloud-computing system.

Cloud-computing links remote computers, so that users can access remote data storage and computation services. It also allows users to increase their effective computing power by tapping into a network of data servers. The potential for cost saving, convenience, and efficiency is tremendous. In addition, cloud-computing gives businesses without the resources to purchase raw computing power, like those in developing countries, the ability to access this power through the cloud, thus helping them compete in the global market.

These computing clouds have grown to include more users across different countries, frequently moving personal data across multiple jurisdictions and inevitably raising concerns over data protection. And in the wake of one the

---

largest data breaches in history, politicians are sure to rally support for new and more restrictive data protection regimes. As legislators in each jurisdiction attempt to pass laws that protect their own constituents, jurisdictional issues arise that threaten the stability of an international cloud-computing regime.

This Comment attempts to analyze and resolve the international law implications of cloud-computing by identifying two possible equilibrium states of a global cloud-computing system. The first state is one in which countries use jurisdictional theories to give their data-protection laws extraterritorial effect. The second state is one in which countries cooperate through an international agreement or organization to find a common solution to the risk of data loss in cloud-computing. Section II begins the discussion by providing background information about cloud-computing and the basic forms of domestic data protection law. This Section also argues that cloud-computing will become increasingly relevant as processor speeds reach certain technological bottlenecks. Section III addresses the first equilibrium state by discussing the viability of different jurisdictional theories that states may use to justify cloud-computing regulation with extraterritorial effect. Section IV addresses the second equilibrium state by describing three ways in which international cooperation may manifest itself. Section V concludes.

II. CLOUD-COMPUTING

Cloud-computing services, offered by cloud-computing service providers (CCSPs), represent a collection of technologies aimed at “allowing access to large amounts of computing power in a fully virtualized manner.” The cloud-computing service is a system by which individuals can access computing power remotely by storing data on centralized servers, as if in a cloud. Perhaps the best example of this kind of service is one that is almost ubiquitous now: web-based email services like Gmail and Hotmail. Increasingly, businesses have turned their attention towards cloud-computing. They see it as a “hyper-efficient means of distributing digital services,” and thus as a potential cost-saving measure. Indeed, lesser-known CCSPs, like Amazon, Cisco, and Microsoft, have catered

4 Id.
to this group by offering not only data storage but computing processing services. In addition, Google has introduced Google Chrome OS, an operating system designed to function almost completely through the cloud, providing essentially remote computing software that can be updated automatically through the web.

There are three main types of cloud-computing services: (1) Infrastructure as a Service (IaaS), (2) Platform as a Service (PaaS), and (3) Software as a Service (SaaS). These form the “layers” of a cloud where the services that are more sophisticated depend on lower layers to function. IaaS includes computation, storage, and communications, and it represents the bottom layer of the cloud. Amazon Web Services, for example, mainly offers IaaS. PaaS refers to a “cloud platform,” which offers an environment where developers create and host web applications. Google App Engine is an example of a PaaS. SaaS is the top layer of the cloud, and it provides users with fully functioning applications that rest entirely on the cloud. Recognizable examples of these services are Google Docs, Google Spreadsheets, and the Chrome OS discussed above.

Importantly, cloud-computing, particularly at the PaaS stage, represents an environment “on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory [those] applications will be using.” When software developers write software for normal operating systems designed to run on computers, applications must be written in such a way so as not to use too much power or memory while also being able to coexist with other applications. With platform cloud-computing, however, developers are able to assume that platforms that run on the cloud can utilize an effectively unbounded processor speed and memory. “Cloud-computing gives the illusion of infinite computing resources available on demand”; thus, such a system requires that “additional resources can be (a) provisioned, possibly automatically, when an application load increases and (b) released when load decreases.”

---


8 Voorsluy, Broberg, and Buyya, Cloud Computing § 1.3 at 13–14 (cited in note 3).

9 Id at 14, § 1.3.1.

10 Id.

11 Id at 15, § 1.3.3.

12 Voorsluy, Broberg, and Buyya, Cloud Computing at 14, § 1.3.2 (cited in note 3) (emphasis added).

13 Id at 16–17, § 1.4.3.
Harnessing the Cloud

A global network of cloud-computing systems would need to function with comparable elasticity, that is, it must be able to move resources across systems as quickly and freely as possible. For example, because of energy consumption concerns at individual data centers, CCSPs require “Dynamic Resource Allocation,” which matches power supply to demand and avoids overheating. In order to run this system efficiently, CCSPs must be able to move data freely between servers, the “nodes” of the cloud-computing system, which will likely be located in multiple jurisdictions. As these CCSPs join together and remove barriers between services, providers will aim to take advantage of efficiencies of scale and offer a wider range of services to an ever-larger geographic region.

Therefore, global or regional CCSPs will inevitably run up against international law, particularly data protection law and privacy regulations. As individual and corporate users of CCSPs put their data on the cloud, they are exposed to the risk of data loss and violations of privacy in exchange for more efficient storage and information access. It may be in the best interest of the CCSPs to minimize that risk, making government intervention unnecessary. Nevertheless, states have stepped in to ensure that loss of citizens’ data is sufficiently deterred.

For instance, the EU’s Data Protection Directive regulates the processing of personal data in the EU. It lays out a set of minimum protective standards and a conflict of laws regime aimed at breaking down barriers between individual nations’ incompatible sets of privacy and data protection laws. At the heart of the Directive, and for the purposes of this Comment, the rules break down into two types: (1) adequacy protections and (2) rights to data. The latter type includes, but is not limited to, the rights to

14 Id.
15 Id at 19, § 1.5.1.
16 See Voorsluy, Broberg, and Buyya, Cloud Computing at 19, § 1.5.1 (cited in note 3).
18 See id at § 1.8.1 at 35.
19 See Dou, Is Europe Ready? at 5 (cited in note 1).
21 See generally id.
22 Compare id at Art 25 (“[A]dequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data
access, correct, and erase personal data. It may also include regulations restricting private data to certain locations or imposing durational limits on the retention of such data exiting the territory.\(^{23}\) Other countries have modeled their privacy regulations after the Directive and thus have similar systems.\(^{24}\)

One may ask whether a close analysis of cloud-computing regulation is relevant in a world in which technology is advancing so rapidly that cloud-computing itself may quickly become obsolete. Though there are cost-saving and data-protection advantages related to the use of cloud-computing services, if better and faster processors and computers are created, cloud-computing will not reach the kind of ubiquity and relevance that would necessitate international cooperation on the issue. However, as many in the semiconductor industry have noted, there are "a set of impending bottlenecks \ldots where more than five decades of progress in continuously shrinking the size of transistors used in computation will end."\(^{25}\) As innovation enabling faster processor speeds and larger memory begins to decline, users will inevitably look to cloud-computing services to increase their effective processing power and storage capacity. If this "bottleneck" is not averted, many industries may come to depend on cloud-computing services as a supplement to, or even a substitute for, their own computing services. Even if a solution to the "bottleneck" is developed, this Comment predicts that cloud-computing will become a public utility because individuals and firms alike will look to the cloud to close the gap between inherently limited non-cloud-computing power and their demand for high computing performance.

\(^{23}\) See Ephraim Schwartz, *The Dangers of Cloud Computing* (InfoWorld July 7, 2008) online at http://www.infoworld.com/d/cloud-computing/dangers-cloud-computing-839?page=0,2 (visited Oct 24, 2011): For example, the European Union places strict limits on what data can be stored on its citizens and for how long. Many banking regulators also require customers' financial data to stay in their home country. Many compliance regulations require that data not be intermixed with other data, such as on shared servers or databases.


III. INTERNATIONAL LAW JURISDICTION FOR CLOUD-COMPUTING REGULATION

As discussed above, existing data protection regulation does not entirely foresee the kind of cloud-computing regime we may expect once cloud-computing becomes a necessary component of production. Yet this kind of regime—in which each country utilizing cloud-computing services establishes its own data protection laws and mechanisms—may represent an equilibrium state of the system. To guarantee stability, however, the individual protection regimes must establish extraterritorial jurisdiction under international law.

This section outlines different jurisdictional grounds under international law that may justify effective cloud-computing regulation. The first part discusses three preliminary assumptions for the jurisdictional analysis: (1) the exercise of extraterritorial jurisdiction is permitted unless existing international law prohibits it; (2) the data protection laws at issue are public rather than private law; and (3) the exercise of jurisdiction is “reasonable.” The second part of this section begins the analysis and concerns both the objective and subjective territorial principle. The third part discusses the nationality principle. The fourth part discusses the passive personality principle. Finally, the fifth part discusses the protective principle.

A. Preliminary Assumptions

The first assumption concerns the ability of states to extend jurisdiction under international law. This type of system is predicated on an international law regime buttressed by the case of *Lotus*, in which the Permanent Court of International Justice determined that there is no restriction on states’ exercise of jurisdiction unless there is international law prohibiting such an exercise. Though the *Lotus* principle has been criticized over the years, the International Court of Justice advisory opinion concerning Kosovo’s unilateral declaration of independence suggests that the principle is still salient. Moreover, because cloud-computing represents a brand new frontier for international law, the principle that everything that is not expressly forbidden is allowed seems more acceptable and perhaps even essential.

With regard to the second assumption, it is important to note that the cases discussed below deal almost exclusively with so-called “public law,” such as criminal and antitrust law. International “private law,” on the other hand, such

26 *Lotus* (Fr v Turkey), 1927 PCIJ (ser A) No 10 (Sept 7, 1927).
28 See id at 68, citing * Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion, ¶ 56 (July 22, 2010).
as tort and property, is mainly determined by conflict of law provisions within contracts. When such provisions are omitted from contracts, conflict of law provisions in public law, like parts of the EU Directive, are meant to determine which laws apply. Data protection is an area of mixed private and public law, so some provisions in certain circumstances may apply as public law. It is neither useful nor imperative to analyze specific regulations in order to determine which provisions are public and which are private. Instead, for the purposes of this Comment, I assume that all regulations may act as public law. Indeed, if these were private laws, they would only have minimum effect, as CCSPs maintain greater bargaining power as utilities and would strive to include conflict of law provisions that would, in equilibrium, bring their activity under the least strict set of laws. If cloud-computing becomes a public utility, as predicted, CCSPs will either not be permitted to contract out of such provisions, or there will be sufficient competition among CCSPs to compete away providers that choose to use conflict of laws provisions to bring their activity under the least restrictive laws.

Finally, all justifications for jurisdiction are necessarily influenced by Section 403 of the Restatement (Third) of Foreign Relations Law. This section provides that “a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable.”

B. Territorial Principle

1. Subjective territorial principle.

States have the power to prescribe public law in their own territory. Historically, this justification has been narrowly used by states to prescribe laws for their own geographic territories. This may be due to the fact that “unrestricted movement of individuals or of property to or from other countries did not in the past occur so readily or frequently as between states bounded for the most part by land frontiers.” More recently, there have been a number of extensions of this principle, as countries cast a wider net in their legislating

---

31 Id at 182.
33 Id at § 402(1)(a).
34 I.A. Shearer, Starke’s International Law 183 (Butterworths 11th ed 1994).
powers in response to other states’ inadequate adjudication of certain matters.\(^3^5\) The subjective territorial principle extended jurisdiction to activities commenced within a state’s geographical territory but completed or consummated in other territories. This is now part of international law with regard to specific realms of activity, namely currency counterfeiting and drug trafficking.\(^3^6\) Though this form of territorial jurisdiction is not widely accepted as a general principle, the Restatement of Foreign Relations Law leaves room for its expanded application. Section 402, entitled “Bases of Jurisdiction to Prescribe,” provides that “a state has jurisdiction to prescribe law with respect to . . . conduct that wholly or in substantial part[ ] takes place within its territory.”\(^3^7\)

In *Treag v DPP*,\(^3^8\) a UK case, the defendant attempted to blackmail a woman in Germany through a letter he wrote in England. The English law stated that a person was guilty of blackmail if he made an “unwarranted demand with menaces.”\(^3^9\) The defendant argued that he made no such demand in England, but the House of Lords disagreed, stating that he made the demand when he wrote the letter in England.\(^4^0\) This is a straightforward example of the subjective territorial principle, in which the activity in question, blackmail, began in England, and even though it was completed or consummated in another territory, English law applied.

In *Ong Ab Chuan v PP*,\(^4^1\) a Singapore case, the defendant appealed a lower court conviction of trafficking heroin. The defendant argued that he was merely carrying the drugs and that there was no evidence of trafficking.\(^4^2\) The court importantly drew a distinction between transporting drugs for one’s own personal use, which was not “trafficking” under the relevant law, and the act of transporting with the intent to distribute, *whether achieved or not*.\(^4^3\) Within the realm of drug trafficking, then, the court took a broad view of the subjective territorial principle. By stating that possessing with the mere intent of distributing, without actual consummation, was still captured by Singapore law, the court endorsed an


\(^3^7\) Restatement § 402(1)(a) (cited in note 32) (emphasis added).

\(^3^8\) *Treag v Director of Public Prosecutions*, [1971] 1 All ER 110 (HL 1970) (UK).


\(^4^0\) Fitzpatrick, 21 Intl & Comp L Q at 160–61 (cited in note 39).

\(^4^1\) *Ong Ab Chuan v Public Prosecutor*, [1981] AC 648 (Singapore).

\(^4^2\) Id at 663.

\(^4^3\) Id at 668.
extension of extraterritorial jurisdiction based merely on intent to commit a crime, suggesting that "commencement" for purposes of the subjective territorial principle may be read broadly.

Countries may find that the subjective territorial principle provides a jurisdictional basis to bind CCSPs to their cloud-computing regulations. Under this line of reasoning, with regard to adequacy measure regulation, when there is harm related to data loss or theft, states can use the entire chain of data—made up of data transfers between servers—to identify specific servers that do not abide by the given adequacy measure. Once identified, the injured country or party could extend that country's jurisdiction to the CCSP controlling the rogue server under the theory that their inadequate protection began with compiling the data from the user in the injured country. Though Ong Ah Chuan suggests that the activity under the purview of the law may be read very broadly, applying such a broad view to data collection could be considered an overextension of the principle. However, concerns over data protection with regard to cloud-computing, which, as discussed above, necessarily requires that data freely move across borders, are similar to those over other activities covered by the subjective territorial principle. Drug trafficking and counterfeiting currency laws both aim to ensure that those who commence such activities cannot escape liability by moving across borders. Similarly, the goal of cloud-computing regulation is to ensure that the CCSPs cannot escape the onus of an adequacy measure or a right to access by moving data across borders. Because the character of these activities is similar, and because international law may be broadened to apply to the accumulation of data, the subjective territorial principle could be used to provide jurisdiction for cloud-computing regulations.

2. Objective territorial principle.

Under the objective territorial principle, the state's jurisdiction is extended to those acts that are commenced in another state's territory but are either (a) consummated or completed in its territory or (b) produce harmful consequences in the territory of the party extending jurisdiction. The first component of this principle is the complement to the subjective territorial principle. Thus, the states of both the blackmailer and the blackmailed in Treacy would have jurisdiction over the defendant. It is difficult to imagine a way in which cloud-computing regulations could be justified under this part of the objective territorial principle. The activity in question, which would most likely be inadequately protecting data, would either have not been completed in the regulating country, putting it outside of the purview of this principle, or would

---

have been completed in the country, placing the CCSP within the purview of the regulation under traditional theories of territorial jurisdiction.

The second component of this principle has come to be known as the “effects doctrine.” This doctrine suggests that jurisdiction arises when the effects of a particular activity are direct and are “so reprehensible [in] nature, . . . economic or otherwise, as to attract or necessitate such jurisdiction.” The seminal case for this principle is the 1927 *Lotus* case. There, the French ship Lotus collided with a Turkish ship. The collision was due to the apparent gross negligence of the officer on watch on the Lotus. It resulted in the deaths of eight Turkish nationals. Turkey brought proceedings against the officer of the watch, a French national, claiming that the negligent act created “effects” on a part of Turkish territory: the boat itself. The Permanent Court of International Justice found that jurisdiction “was not inconsistent with international law.”

Since this ruling, other countries, including the US, have recognized extraterritorial extensions of jurisdiction based, implicitly or explicitly, on the effects doctrine. In the *Wood Pulp* case, for example, the European Commission fined two trade associations with registered offices in Canada, Finland, Switzerland, and the US for violating European Economic Community (EEC) laws prohibiting price-fixing, exchanges of information on prices, and the export or resale of wood pulp from the EEC. The trade associations argued that the Commission had no jurisdiction to impose the fines, and the central question for the European Court was whether the “effects doctrine” could be justifiably applied. Though the Court declined to expressly invoke or endorse the effects doctrine, it upheld jurisdiction on narrow grounds. The Court utilized a principle known in the EU as the “implementation requirement.” Under this principle, states are only justified in using the effects doctrine when those effects are “intended, direct and substantial.” Though similar to the effects doctrine, this heightened standard demanding that effects be more closely tied to the state

---

45 Id at 663.
46 Id at 662.
47 Id.
49 Lowe, 48 Camb L J at 9 (cited in note 48).
50 Id at 10.
51 Id.
extending jurisdiction is crucial in determining the breadth and scope of cloud-computing regulation. 53

One area of regulation that may shed light on the treatment of cloud-computing regulation under international law is legislation concerning content on Internet websites. In the *Yahoo! Case*, 54 the dispute centered on Nazi-related items available on the Yahoo! auction site, allegedly in violation of a provision in the French penal code prohibiting the selling of such items. The Tribunal de Grande Instance found that French courts did have jurisdiction because the placement of items for sale “caused damage to be suffered by La Ligue Contre le Racisme et L’Antisemitisme and l’Union des Etudiants Juifs de France, two organizations dedicated to fighting anti-Semitism.” 55 Since both of these organizations were in France, the Tribunal reasoned, France had jurisdiction to hear the case. On appeal, Yahoo! claimed that France did not have jurisdiction, because all of the elements that made up the offense in question were committed outside of France. 56 The Tribunal concluded, however, that because the content was available in French territory through the Internet, the elements “materialized” both abroad and in France. 57 Similarly, in a German case, *Toben*, concerning an Australian who expressed revisionist views of the Holocaust, the Federal Court of Justice found that an element of the offense in question, “agitation of the people,” had occurred in Germany, and thus that German jurisdiction was valid. 58

With this understanding of the effects doctrine, as well as its more onerous cousin, the implementation requirement, one may determine whether this incarnation of the objective territorial principle may be used to provide jurisdiction for cloud-computing regulation. The argument for jurisdiction under the effects doctrine component of the objective territorial principle is straightforward. In the event of a violation of a state’s data protection or privacy laws, the state seeking to extend jurisdiction would argue that the harm suffered was an “effect” of the violation, even if that act was committed wholly outside of the state’s territory. Under this reasoning, a failure either to meet adequacy

53 See id at 288.
54 *UEJF v Yahoo! Inc*, TGI Paris, Ordonnacede Référe, Nos 00/05308, 00/05309 (May 22, 2000) (*Yahoo! Case*).
55 See *Yahoo! Inc v La Ligue Contre Le Racisme Et L’Antisemitisme*, 433 F3d 1199, 1225 (9th Cir 2006), discussing the *Yahoo! Case*.
57 Id at 293.
58 Id at 295, quoting LG Mannheim, Urt v 10.11.1999–5KLs 503 Js 9551/99 (1999) (Ger) (*Toben Case*).
standards or to provide rights to data causing economic harm to individuals or business entities in the state implicates the regulation. This argument is buttressed by the fact that courts, as in the Wood Pulp case, have considered economic harms sufficient to trigger jurisdiction under the effects doctrine.\(^5\)

One may argue that unlike the economic harms suffered in the antitrust cases such as the Wood Pulp case, in which the effects doctrine seemed to be implicated, some of the potential harms related to loss of data (or more appropriately loss of control over data) are less pecuniary. These harms include emotional distress due to loss of private data and other inchoate harms. Thus, under a heightened “implementation requirement” standard, there is a question as to whether these non-pecuniary harms would be “substantial” enough to invoke the effects doctrine as a basis for extraterritorial jurisdiction. However, in the internet cases, Yahoo! and Toben, the harmful effects felt inside the territories of France and Germany were non-pecuniary and abstract, yet the courts upheld jurisdiction under the effects doctrine.\(^6\)

This is not to say, however, that if more abstract harms are insufficient to trigger the effects doctrine, there are no other injuries related to a violation of a cloud-computing regulation. There are potential harms, such as loss of profits by a corporation, identity theft, and loss of trade secrets, that are classic and tangible economic harms. Even assuming that the effects doctrine cannot provide a jurisdictional basis for non-pecuniary harms, existing applications of international law suggest that a state has jurisdiction over activities abroad that cause measurable harmful effects in that state. Thus, under international law, states could enjoy at least a narrow justifiable extension of jurisdiction over violations of cloud-computing regulations under the effects doctrine.

C. Nationality

The power of states to prescribe laws covering the activities of its nationals is uncontroversial and is recognized by the Restatement.\(^6\) Under the active nationality principle, an iteration of the nationality principle discussed in this section, a state has jurisdiction over proceedings against any of its nationals. “The active nationality principle is generally conceded by international law to all states desiring to apply it.”\(^6\) This principle, then, provides states with the ability to prescribe cloud-computing regulations for their nationals at home or abroad.

---

\(^5\) See the Wood Pulp Case (maintaining jurisdiction over the extraterritorial activities of foreigners that caused economic consequences within the territory under a narrowed version of the effects doctrine) (cited in note 48).


\(^6\) See Restatement § 402(2) (cited in note 32).

However, there are disagreement and controversy over the definition of “corporate nationality.” Under one definition, and generally under US practice, a corporation is a national of the state in which it is incorporated.63 There are also instances in which the US has extended nationality jurisdiction to corporations “owned or controlled” by US citizens.64 This includes subsidiaries of US companies incorporated abroad. If this is a legitimate extension of nationality jurisdiction under international law, one can imagine an equilibrium solution to a system of domestic cloud-computing regulations with international reach. In this system, CCSP corporations include equity holders from all countries utilizing that particular provider. If a CCSP did not meet adequacy measures or sufficiently honor rights to data, nationality jurisdiction would allow injured states, through equity holders, to bring that CCSP under domestic laws to adjudicate the matter. This kind of solution might be particularly attractive because it would require no explicit agreement between nations, only an understanding that, under international law, nationality jurisdiction extends to corporations in which states had a sufficient amount of equity.

However, there are cases that suggest such an extension of nationality jurisdiction is not recognized under international law. When the US has extended jurisdiction in this way, for example, it has spurred protests and countermeasures in foreign countries, as well as rulings in favor of those states.65 In Compagnie Europeanne des Petroles SA v Sensor Nederland BV,66 a French corporation placed an order with a Dutch corporation that subsequently was bought by an American corporation. The order was destined for the USSR. After Sensor became a subsidiary of the US corporation, it claimed that it was bound by a US export embargo to the USSR and reneged on the deal.67 The District Court of the Hague considered and rejected extraterritorial jurisdiction based on the nationality principle. The court stated that even if the embargo’s language giving itself jurisdiction over corporations “owned or controlled” by American nationals was a “yardstick for the (U.S.) nationality of the corporation,” the idea of nationality jurisdiction’s extending to such parties, according to views held outside the US, was “dubious.”68

63 See id at 685.
64 See id.
65 Id at 686. See also id at 695–702 (discussing hostile international reactions to the Helms Burton Act).
In the case of *SA Fruehauf*, a French corporation 70 percent American-owned and 30 percent French-owned won a bid to supply a large number of trailers to a French company. When the US learned that the trailers were bound for China, they ordered Fruehauf to cancel the order in accordance with the Trade with the Enemy Act. The three French directors of the company petitioned a French court to appoint an administrator that would take control of the company and carry out the contract, implicitly soliciting the court to exercise its own nationality jurisdiction over Fruehauf. The French courts obliged, and the case eventually resulted in additional French legislation designed to protect national corporations from foreign control. A later case, *Dresser*, which involved a similar set of facts, also ended with the host nation prevailing over foreign (or home country) interests.

As these cases suggest, an extension of the nationality principle to prescribe laws for corporations in which nationals merely have an equity interest is heavily resisted, and it may not be a recognized extension of jurisdiction under international law. But this limitation on jurisdiction may also have the effect of encouraging international cooperation. Given the fact that the largest CCSPs are US entities (for example, Amazon and Google), the limitation on nationality jurisdiction would constrain the US’ ability to prescribe cloud-computing regulations for all world users of these CCSPs. Limiting the US’ extraterritorial jurisdiction in this way prevents the US from dictating the relevant terms of a global cloud-computing regulatory scheme. Thus, if these CCSPs want to have subsidiaries in the countries they service, which they likely will, those corporations would be subject to the host country’s regulations.

D. Passive Personality

The passive personality, or passive nationality, principle provides jurisdiction to a state for foreign activities that cause injury to nationals of that state. This principle is most frequently applied in response to terrorist attacks. In the 1887 *Cutting* case, a US citizen was charged with criminal libel in Mexico

---


72 See text accompanying note 63.

after publishing an article criticizing a Mexican citizen. Though the case was resolved through diplomatic means, and the Mexican court that convicted Cutting did not discuss whether the passive personality principle could be a basis for doing so, the incident did result in a US Department of State letter that explicitly stated that the passive personality principle was not a basis for extraterritoriality jurisdiction.

This view remained dominant in the US for over a hundred years. In the *Lotus* case, discussed above, the statute Turkey used to justify jurisdiction provided that “[a]ny foreigner who ... commit[ed] an offence abroad to the prejudice of Turkey or of a Turkish subject” would be subject to Turkey’s jurisdiction. Though the majority opinion by the Permanent Court of International Justice did not discuss passive personality jurisdiction, a dissenting opinion argued that customary international law did not permit it. This notion was reflected in the Convention on the High Seas of 1958, which provided that “only the flag state or the responsible officer’s home state could prosecute the officer for collisions or other incidents of navigation on the high seas.”

Yet in more recent years the US has appeared to use the passive personality principle as a basis for jurisdiction in the realm of terrorist crime, by signing on to international agreements like the Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, which arguably reflect the principle. Some commentators argue, however, that the actuating principle in these agreements is the protective principle, discussed below. In 1984, the US Congress passed legislation to implement the Convention Against the Taking of Hostages, which provided that even if an offense was committed outside the US, the statute would apply if the offender took a US national hostage. In 1992, Congress passed a measure to make international terrorism a federal crime. The legislation also provided civil remedies for “[a]ny national of the United States injured in his or her person, property, or business by reason of an act of international terrorism.” Though one may argue that the jurisdictional theory upon which these pieces of

---

75 Id.
76 Id at 302–07.
78 Id at 8.
79 Id at 9.
80 Id.
legislation are based is the protective principle, not the passive personality principle, the statutory language suggests that the conduct that triggers jurisdiction is an act against nationals.\textsuperscript{83}

The first obstacle to the use of this principle in justifying extraterritorial jurisdiction for cloud-computing regulation is determining whether the passive personality principle can reasonably be extended outside of the criminal context. The central question here is whether the injuries that may result from inadequate data protection are the kinds of harms that justify protection under the passive personality principle. Some of the more straightforward economic harms, such as a company's losing profits due to data loss, are so different from the harms used to justify the principle that, at present, international law would likely not support its use in this context. There are other harms, however, such as violations of individual privacy—a principle recognized by the UN as a human right—that may be sufficiently severe.\textsuperscript{84} Thus, similar to the discussion concerning the effects doctrine, one could argue that jurisdiction for cloud-computing regulations under the passive personality principle would arise on a case-by-case basis, when the resulting harms were significant enough. States would use this form of extraterritorial jurisdiction to protect their nationals against CCSPs that injure them by violating adequacy measures or by insufficiently protecting rights to data. Moreover, given that it might be difficult to determine exactly where these harms occur (for example, when data is transferred through multiple servers across different jurisdictions) and given that the country in which the service is incorporated may not have great incentives to bring actions against the CCSP, cloud-computing regulations may be an ideal application of the passive personality principle.

E. Protective Principle

States may also exercise extraterritorial jurisdiction over activities that affect vital security or economic interests.\textsuperscript{85} The Restatement (Third) of Foreign Relations Law provides that a state has jurisdiction to prescribe law with respect to "certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests."\textsuperscript{86} Comment (f) of the Restatement describes this "limited class" as "offenses threatening the integrity of governmental functions," such as

\begin{footnotesize}
\textsuperscript{83} See id.
\textsuperscript{84} See International Covenant on Civil and Political Rights, Art 17, 999 UN Treaty Ser 171 (1966) (ICCPR) (recognizing a right to privacy).
\textsuperscript{86} Restatement § 402(3) (cited in note 32).
\end{footnotesize}
"espionage, counterfeiting of the state's seal or currency, falsification of official documents, as well as perjury before consular officials, and conspiracy to violate the immigration or customs laws." These are situations where the offense in question was sufficiently grave so as to implicate an important interest of the state, as well as situations where without such jurisdiction the offense would not be punished. As noted in the preceding section, given the logistics of a cloud-computing service, one might expect that the place of the offense would be difficult to identify and that the home country may not have the proper incentives to punish violations of cloud-computing regulations. This argument notwithstanding, there are likely only a very limited number of situations where cloud-computing harms would implicate national security issues or rise to the level of the "limited class." There are instances in the law of the sea, however, that suggest that the protective principle is used to extend jurisdiction to matters outside of criminal offenses. In Article 65 of the UN Convention on the Law of the Sea (UNCLOS), parties to the Convention are permitted to "regulate the exploitation of marine mammals" in an exclusive economic zone, a defined area off the coast of a state. But Article 120 extends this right to the high seas. Though this does not grant states jurisdiction over marine mammals in other states' extended territory under the treaty, it arguably represents extraterritorial jurisdiction justified by the protective principle in a non-criminal context.

States that use the protective principle to extend jurisdiction to CCSPs must argue that those extraterritorial activities threaten vital economic or security interests of the state. As individuals continue to utilize cloud-computing services, more and more sensitive data are likely to be stored in the cloud. A state may argue that under such circumstances, CCSPs that do not adequately

87 Id at comment (f).
91 See id at Art 120.
Harnessing the Cloud

Narayanan

protect data pose a serious threat to the interests of the state. Though the threat would likely not rise to the level of a vital security interest in the same vein as terrorism, a state in which a majority of individuals utilize cloud-computing services could reasonably argue that data security is of vital economic interest to the nation. As a consequence, the state would find it necessary to extend extraterritorial jurisdiction to these activities, en masse, without a finding of specific harm or a showing that the CCSP has nationality. Thus, the protective principle, unlike some of the jurisdictional principles discussed above, would allow states to extend jurisdiction to these activities without predicing that jurisdiction on the specific circumstances of the case, such as whether there were harms associated with the activity. For this reason, if cloud-computing becomes sufficiently ubiquitous and if the “limited class” of activities under the protective principle expands, this principle could be a valuable form of extraterritorial jurisdiction for states that use cloud-computing services.

IV. INTERNATIONAL COOPERATION

As the preceding Section indicates, international law may provide a jurisdictional basis for states to prescribe cloud-computing regulation with extraterritorial effect. But even with this ability, one may question whether a system in which individual states exercise this kind of jurisdiction over CCSPs would be efficient. CCSPs would have to navigate through a web of regulations, ensuring that their systems abide by the highest level of adequacy measures and right-to-data regimes. This would be costly and unstable, as states may initiate a kind of race-to-the-top and attempt to ensure that their regulations are controlling by making them the most restrictive. In addition, as discussed below, existing international agreements may constrain the ability of states to regulate these services at too high or too low a level. Given these problems, an ideal solution for cloud-computing regulation, in a world in which cloud-computing has become prevalent, is international cooperation.

Ultimately, this cooperation may manifest itself in different forms. Cooperation may be achieved by utilizing existing international organizations, such as the UN or the WTO, to harmonize cloud-computing regulations and set minimum standards; states would have to meet these standards or be subject to enforcement mechanisms already in place. Another manifestation may be a wholly new international organization, which, instead of simply harmonizing regulations or setting minimum standards, would be organized such that it could actively promulgate regulations as cloud-computing service technologies inevitably change. Finally, cooperation may manifest itself through an agreement that divides up the relevant “space” inside the cloud to ensure that specific areas are governed by specific sets of regulations. This would be akin to a type of law of the sea for the computing cloud, which ensures that jurisdictions are
demarcated and that regulatory powers are cabined off in specific areas to prevent jurisdictional clashes.

The first part of this Section discusses ways in which existing international agreements may constrain the ability of states to regulate cloud-computing service providers. The second part considers the possibility of international cooperation in the form of a harmonization of cloud-computing regulations akin to the Agreement on Trade-Related Aspects of Intellectual Property (TRIPs). The third part examines the possibility of a unique international organization dedicated to promulgating or evaluating cloud-computing regulations. The final part considers a system in which cloud-computing service providers are subject to different laws in different parts of the cloud “space,” and it uses the UN Convention on the Law of the Sea as an analytical tool in this regard.

A. Constraints on Cloud-Computing Regulation

The first constraint on a state’s ability to regulate computing clouds is derived from a WTO agreement concerning free access to services. The constraint seems to place an upper bound on the level of regulation. The WTO envisions a system of free trade that allows free supply of services across member states. This principle is reflected in the General Agreement on Trade in Services (GATS), which discusses four different “modes” of service supply: (1) cross-border supply, covering services flowing from the territory of one state into another; (2) consumption abroad, covering services that have consumers moving from one territory into another to utilize a service; (3) commercial presence, covering service providers of one territory that create a presence in the territory of another; and (4) presence of natural persons, covering individuals of one territory going into another territory to provide a service. Importantly, GATS also requires all members provide “treatment no less favourable than that it accords to like services and service suppliers of any other country.” These requirements, however, are subject to a broad set of general exceptions that must be applied reasonably. The exceptions state that nothing in the Agreement prevents measures that are “(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions . . . relating to . . . (ii) the protection of the privacy of individuals in relation to the processing

95 GATS, Art 2. See also GATS Objectives (cited in note 89).
96 GATS, Art 14.
and dissemination of personal data and the protection of confidentiality of individual records and accounts[.]

CCSPs would undoubtedly fit into one of the “modes” of supply that the GATS agreement purports to cover. The service providers, depending on how this kind of data transfer is characterized, may be described as providing services from one territory to another, as drawing consumers to their “territory” to obtain cloud-computing services, or as creating a presence in another’s territory to provide the cloud-computing service. If cloud-computing services do qualify as one of the modes, member states would be required to comply with the prohibition on providing favorable treatment to services from one state over another, subject to the general exceptions. Favorable treatment may arguably include having adequacy requirements that are onerous for foreign CCSPs. Because of the level of interconnectedness on which cloud-computing depends, measures that are especially burdensome in one territory may make it infeasible or unprofitable to provide transborder services in that area, forcing customers to rely on national CCSPs that do not move data across borders. The EU Data Protection Directive, for example, includes a provision that requires an “adequate level of protection” of data before a transfer to a “third party” outside of the EU. Of course, the EU or states with similar protections would argue that these regulations would be permitted under exception (c) because the measures are specifically designed to protect privacy. But these exceptions must be applied reasonably. Thus, the exception does not function as a carte blanche for states; they are still prohibited from providing more favorable treatment to regional CCSPs over foreign ones, unless the regulations are reasonably designed to protect individuals’ privacy. Some commentators note, for example, that the Directive provision discussed above may favor services from EU nations over US service providers in a way that would not be reasonable.

---

97 Id.


99 See Krishnan Subramanian, Cloud Vendors Plead for Uniform Regulations in Europe (CloudAve July 30, 2010), online at http://www.cloudave.com/98/cloud-vendors-plead-for-uniform-regulations-in-europe/ (visited Oct 24, 2011) (“One of the reasons for the failure of public cloud providers . . . is the strict privacy laws that requires the cloud providers to keep the data within the borders.”).


101 See generally Asinari, WTO and the Protection of Personal Data (cited in note 98).
The second constraint seems to provide a lower bound to regulation. It is triggered by the UN’s International Covenant on Civil and Political Rights and its protection of a right to privacy.102 A 2010 report from a UN Special Rapporteur assisted by the Office of the High Commissioner for Human Rights, concerning the protection of privacy rights while countering terrorism, elucidates these constraints.103 The report underscores the importance of a right to privacy in the realm of data protection by calling for “a comprehensive data protection and privacy law . . . to ensure that there are clear legal protections for individuals to prevent the excessive collection of personal information . . . [; to] create[] limits on the use, storage, and sharing of the information[,] and [to] mandate[] that individuals are notified of how their information is used and that they have a right to access and redress, regardless of nationality and jurisdiction.”104 The recommendations also call for strong oversight when personal data are collected.105 Though the crux of the report concerns government anti-terrorism measures such as wire-tapping, the right to privacy is the actuating principle for the call to reaffirm individual rights in data.106 Moreover, the report notes in its examination of the right to privacy that “data protection is also emerging as a distinct human or fundamental right.”107 Thus, it is reasonable to argue that even outside the terrorism context, this “fundamental right” requires a certain level of protection. Though states may not be required to comply with the recommendations of the Office of the High Commissioner with regard to cloud-computing regulations, the report suggests that the right to privacy at least requires a right to data protection as well.

B. Harmonization

International cooperation for cloud-computing regulation may come in the form of an agreement to harmonize data protection laws. Like the TRIPs agreement, the WTO could convene members to examine the issue and determine the basic standards of data protection laws that would be optimal. With the TRIPs agreement, the danger posed by a lack of harmonization meant that companies that owned intellectual property (IP) were wary of globalizing the use of their technology or copyrighted works because of the risk of

102 See ICCPR, Art 17 (cited in note 84).
104 See id at ¶ 61.
105 See id at ¶ 62.
106 See id at ¶¶ 11–20.
misappropriation. This risk was compounded when the IP was moved into countries that did not have a sufficient level of protection. A similar concern would exist with cloud-computing regulation. When a piece of data moves through different territories, there is an increased risk of loss in countries that do not require sufficient protections for data storage or transfers. Thus, a harmonization agreement would impose minimum standards of protection to facilitate the free trade of cloud-computing services.

Unlike other harmonization agreements, however, an agreement to harmonize cloud-computing regulations may pose a unique challenge in its need also to prevent excessive regulation. With regard to IP, developing countries that tend to produce fewer patented technologies or copyrighted works than they use have an incentive to keep IP protection low, in order to maximize access to technology. With regard to cloud-computing, states have an incentive to protect their citizens' data to the greatest extent possible, with the highest level of protection. The only limiting factor here would be if the regulations were so onerous that the CCSPs would not provide service to particular areas. This kind of action might also have consequences in light of GATS, if not implemented reasonably. Even if these CCSPs provide service, though, excessive levels of data protection laws have negative externalities on the system if technology or software has to be updated at multiple nodes in several countries. Thus, a group convened to determine proper standards of harmonization should also determine what the appropriate level of regulation might be—that is, the optimal level for sufficiently protecting private data while also giving CCSPs the latitude to move data freely when necessary to increase the efficiency of the system.

One group tasked with a similar objective is Working Group VI of the UN Commission on International Trade Law. This group's goal is to provide a legislative guide for secured transactions law in order to harmonize the disparate rules of individual countries. The justification for this harmonization is that secured transactions would benefit from a reduction in the transaction costs of providing capital to foreign companies. With a set of common ordering rules, firms would be able to lend with a full understanding of their rights to collateral, without having to learn a different set of rules and without being concerned that the rules would change if collateral were transferred to another country. In addition, "when countries face[] crises in their financial sector, an effective and predictable legal framework [is] necessary... In the longer term, a flexible and effective legal framework for security rights could serve as a useful tool to

increase economic growth.”110 Furthermore, the working group notes that one of the driving forces behind the initiative is to establish modern secured credit laws in order to “alleviate the inequalities in the access to lower-cost credit between parties in developed countries and parties in developing countries, and in the share such parties had in the benefits of international trade.”111 Because cloud-computing has the potential to create similar distribution effects by providing developing countries with access to more computing power than they might be able to have on their own, there may be a similar impetus for global harmonization of cloud-computing regulation.

C. International Regulatory Organization

International cooperation over cloud-computing could be achieved through an international organization specifically dedicated to regulating this type of activity. There are very few analogies to this kind of arrangement, and there are none of the scale that might be necessary to regulate data protection effectively across many different countries. What would be required under this type of system is a delegation of power, wherein the countries utilizing cloud-computing services would agree to allow this international body to provide oversight of the CCSPs. A call for these kinds of organizations is not new. Most recently, in the wake of the 2008 financial crisis, European leaders called for an international financial regulatory body to ensure “cross-border supervision of financial institutions; shared global standards for accounting and regulation; [and] a more responsible approach to executive remuneration that rewards hard work.”112 The advantage of having an international organization dedicated to the task of cloud-computing is that it would be nimble enough to keep up with rapidly changing technologies. Rather than having to force a meeting of members of the WTO, an international CCSP regulatory body would be technocratic in nature and help keep the system running smoothly.

D. The Cyber Sea

The final way that international cooperation could manifest itself is through an international agreement of a different character than TRIPs or the UNCITRAL agreement with regard to secured transactions law. UNCLOS is a treaty designed to codify and change, where necessary, the customary law of the

110 Id at ¶ 2.
111 Id at ¶ 1.
Harnessing the Cloud

sea. The agreement addresses the problem of disputes over sea territory off of states’ territorial borders. It also staves off a tragedy of the commons by delineating clear boundaries near coasts, and it dictates “exploration and exploitation of [the area of the sea-bed and ocean floor] shall be carried out for the benefit of mankind as a whole.” 113 Essentially the agreement makes jurisdiction in extraterritorial areas, like the exclusive economic zone, clear where there is consensus. But importantly, it recognizes that the open ocean, or high seas, is an area under no particular state’s jurisdiction: “The high seas are open to all States, whether coastal or land-locked.” 114 When there are incidents, such as a collision, jurisdiction is determined through the nationality of the ships or the persons in their service. 115

A similar international system may be envisioned for cloud-computing regulation. The computing cloud may be described in completely corporeal terms as a system of linked servers and computers connected through wires and radio signals. Under this conception, data are simply packets of information sent from one jurisdiction to another. But the cloud may be described differently by pointing out that though data exist on specific servers, they may be accessed and transferred to different servers at rapid speeds. In this way, one can imagine the computing cloud as a sea of information, flowing freely from node to node but difficult to pin down into a specific jurisdiction. Data moving from one country to another go through this “cyber sea” to reach their destination. Like the sea, too, there are bad actors. Pirates, traffickers, and smugglers take advantage of the free flow of information to commit crimes like data theft. 116 Similarly, then, a UNCLOS-type agreement could be set up for cloud-computing to divide the system up by giving countries complete jurisdiction over those features of the computing cloud that are “close” to their territory. Just as UNCLOS, in some ways, cemented countries’ jurisdiction extensions into the sea but limited such an expansion, a “cyber sea” agreement would bless certain jurisdictional extensions, justified by the theories put forth in the Section III, while allowing the “cyber sea” to become an area unencumbered by innumerable jurisdictional rules. Unlike UNCLOS, these extensions would not be delineated by physical boundaries, but rather would be determined by the subject matter of the data at issue. Under such an agreement, countries would be permitted to extend their

113 UNCLOS, Preamble (cited in note 90).
114 Id at Art 87(1).
115 Id at Art 97.
data protection law extraterritorially when the data loss at issue is deemed highly private (for example, Social Security Numbers) or particular to that country. Otherwise, when there are incidents that result in data loss, the crime or act of negligence may be said to have occurred on the "cyber high seas." For these situations, the agreement would establish conflict of law rules to determine who would have jurisdiction. Such a system would require a clear ex ante understanding of how these boundaries function, but once in place, the system might find stability by empowering each state to concern itself over its own jurisdiction, while encouraging all states to be aware of and cooperative about solutions for the open waters of the "cyber sea."

V. Conclusion

Cloud-computing represents a set of technologies that, though new and untested, have the potential to change the way people use and interact with data. As the growth of processor speeds and storage capacity slows with impending technological bottlenecks, users will find it necessary to look to cloud-computing to fulfill ever-growing performance demands. In a world of globalized commerce, the necessity of a global cloud-computing regime will become increasingly evident.

This Comment has discussed the viability, under international law, of two possible equilibrium states of an international computing cloud. The first is one in which all countries using cloud-computing services employ extraterritorial jurisdictional theories to impose their own data protection laws abroad. Though case law is scarce, by analogizing from the cases that discuss these principles, jurisdictional theories such as the effects doctrine and the passive personality principle can be used to give cloud-computing regulations extraterritorial effect. The second equilibrium state is one in which countries work together, through an agreement or international organization, to design a common set of data protection laws or to minimize jurisdictional clashes by essentially divvying up the "cloud."

Either system would facilitate the use of the technology and thus would create the right environment for a global computing cloud to emerge. The second of these systems, however, has the vital advantage of allowing a global computing cloud to grow without the constraints of a thicket of data protection regulation. Further, a "cyber seas" agreement may be the ideal vehicle for this kind of system because it provides a balance between a state's ability to regulate the cloud and an overseeing international authority. Regardless of the mode in which this kind of consensus manifests itself, action taken now, while the technology remains nascent, could enable the technology to reach its full potential and be efficiently executed, perhaps even providing unforeseen benefits. Thus, taking the prudent steps now to harness the cloud may, in the
near future, allow the world to reflect on an entirely man-made, global public utility and the beginnings of a truly cooperative world market.