“CLOUDY” SKIES, BRIGHT FUTURES?
IN DEFENSE OF A PRIVATE
REGULATORY SCHEME FOR
POLICING CLOUD COMPUTING

Carol M. Celestine

TABLE OF CONTENTS

I. Introduction................................................................. 142
II. Background............................................................... 144
   A. From ARPANET, to Internet, to the Cloud....................... 144
   B. The Cloud Darkens...................................................... 146
   C. A Wrinkle: Data Sovereignty? ...................................... 148
III. Analysis................................................................. 149
   A. EU Response to the Cloud............................................ 150
   B. Principled? Or Problematic? ........................................ 150
   C. The U.S. Response to the Cloud..................................... 153
   D. Why the Divergence? .................................................. 156
   E. Importance? ............................................................. 157
IV. Recommendation ....................................................... 158
   A. Minimizing Direct Cloud Governance .............................. 158
   B. Utilization and Strengthening of Existing Statutory
      Frameworks............................................................... 159
   C. Policing the Cloud Through Private Norms and Customs....... 160
   D. No Mandated Geolocation of Cloud Data and Data Centers..... 162
V. Conclusion............................................................... 163

“The proper artistic response to digital technology is to embrace it as a
new window on everything that’s eternally human, and to use it with passion,
wisdom, fearlessness, and joy.”—Ralph Lombreglia

* J.D., University of Illinois College of Law, 2013 (projected); B.A., Political Science, Brown
University, 2008. I would like to thank Prof. Jody M. Endres, Mustafa Neak ’12, and my family for their
invaluable support to me during the note writing process. I mean it when I say that it would have been
impossible without them.
I. INTRODUCTION

The era of the impregnable nation state is dead. While sovereignty nonetheless remains more or less intact in its wake, the traditional concept is now challenged by the realities of a world that is becoming increasingly global and borderless. This is a world where citizens seek interactions beyond borders as a matter of course. Though the continuing vitality and importance of national sovereignty is uncontested, the reality is that technological advances have effectively transformed the transactional lives of world citizens.¹ No longer are dealings conducted primarily with intrastate actors on a one-on-one basis. The Internet is now used to conduct dealings electronically and impersonally, dealing with a number of different actors in far flung places, often simultaneously.² This shift from the purely national to the transnational is one of epic proportions. As the Internet continues to expand and transform, these dealings will only become more complicated and implicate more pressing questions of what it means to be sovereign in a global world. Cloud computing presents our newest challenge in this arena.

As the march of technological progress continues, novel additions to the computing canon are constantly coming into existence.³ These developments revolutionize computing, making it more accessible, affordable, and user-friendly.⁴ Cloud computing is one such development. Computing is presently in the midst of a seismic shift from traditional mainframe and client-server-based computing⁵ to the “cloud”—a model that reduces the need for Internet technology (IT) hardware while rendering user information stored in remote locations infinitely more accessible.⁶ Computing has had a significant trajectory, and cloud computing is far from being computing’s first evolutionary phase.

The current transition from client-server computing to cloud computing is similar in form to the technological shift from the cumbersome mainframe delivery model to the client-server model made during the 1980s.⁷ In like form, cloud computing has made IT more decentralized and cost effective than it was during the preceding computing (i.e., client-server) era.⁸

But what precisely is cloud computing? Cloud computing is defined as

---

⁴. Id. at 361.
⁵. Id. at 362 (explaining that the mainframe model involved users operating on slices of a central server’s time rather than maintaining physical control over their files and data) (quotations omitted).
⁶. Id. at 361.
⁸. Id.
being “the delivery of computational resources from a location other than the one from which [the user] is computing.” This novel computing model has become an integrated part of various aspects of daily life, and cloud services are utilized almost constantly, whether or not users realize this fact. Each Facebook login is an entry into the cloud, every Twitter tweet is made possible because of cloud infrastructure. Many household name companies including Google, Microsoft, and Amazon currently provide cloud services.

Above all, the cloud is convenient. At a most basic level of functionality, cloud computing enables users to read emails anywhere and at any time. It makes it possible for multiple individuals in various locations to alter one document. It enables health care providers to access patient medical records with ease. It even permits us to save items to an online shopping cart from one computer and then access the same cart from another. Even the U.S. government has floated into the cloud. From the sublime to the pedestrian, cloud computing vastly enhances computing capabilities and has enormous growth potential: some predict that this potential will be to the tune of approximately $176.8 billion. Though this cloud may be silver-lined, the skies are nevertheless dark. There are unresolved questions of law surrounding cloud policing, governance, and data sovereignty that must be addressed. Tensions have already arisen between nations in regards to the question of which nations’ laws govern data maintained in the cloud. It appears as though cloud computing’s very appeal—its capacity to maintain infinite amounts of data remotely—has become a source of contention between nations.


12. Id.


15. Id.


20. See Jennifer Baker, EU Upset by Microsoft Warning on U.S. Access to EU Cloud, COMPUTERWORLD (July 5, 2011, 12:28 PM), http://www.computerworld.com/s/article/9218167/EU_upset_by_Microsoft_warning_on_U.S_access_to_EU_cloud (describing the European Union’s reaction to learning that Microsoft was unable to guarantee that the data of citizens utilizing Microsoft’s cloud services would not be subject to release under the USA PATRIOT Act).

21. Id.
In response to the growth of cloud computing, the United States and the European Union (EU) are attempting to enact legislation aimed at defining the metes and bounds of the cloud. But will increased regulation truly be effective in structuring the cloud in a manner that will recognize its uniqueness while being sufficiently flexible to accommodate the cloud’s inexorable growth? It is unclear whether this will be the case.

This Note will argue that the interests of maintaining a (relatively) bureaucracy-free cloud must be balanced with the need to develop a basic framework for cloud governance. This can be accomplished by recognizing that governments do have a role to play in cloud governance, but that involvement should be limited to control of data sovereignty while permitting private markets and private actors—using common law contract, tort, informed consent, and disclosure regimes—to determine other jurisdictional, security, and privacy issues. Such an approach will also have the benefit of allowing the computing industry the latitude necessary to engage in the sort of research and development of security technology that will ultimately be capable of dealing with the privacy issues arising as a result of the cloud’s omnipresence.

Part II of this Note will discuss cloud computing’s evolution from the Internet’s inception to its present incarnation, provide a brief explanation of the technology, and discuss the data sovereignty concerns posed by cloud computing. Part III of the Note will analyze existing U.S. and European statutory frameworks governing electronic communications, prospective legislation, and the impact that such frameworks have currently and will have in the future on a growing cloud. It will also explore the possible explanations for the regulatory divergences between the EU and the United States in regards to cloud computing. Part IV will recommend that contract and tort law can be used to draw the contours of the cloud and allocate responsibilities between consumers and providers within the cloud.

II. BACKGROUND

A. From ARPANET, to Internet, to the Cloud

Far from having the transnational reach it enjoys today, the Internet began its life in 1969 as a military research project funded through the Advanced Research Project Agency. The project was dubbed ARPANET. Some trace ARPANET’s conceptual beginnings to as early as 1957, when the United States, spurred to action by the Soviet Union’s launch of Sputnik, embarked on ambitious military research and defense programs to maintain a competitive

24. Id.
technological edge. Initially, the scope of ARPANET’s reach was very limited, connecting mainframes in only five sites: the University of California at Los Angeles, Stanford University, the University of California at Santa Barbara, the University of Utah, and the offices of Bolt, Beranek, and Newman, a small scientific research company in Cambridge, Massachusetts staffed primarily by graduates of the Massachusetts Institute of Technology.

At ARPANET’s inception, mainframe computer systems had only limited data exchange capabilities and were able only to exchange with mainframes of identical manufacture: for example, IBM mainframes could only exchange data with other IBM mainframes, and General Electric mainframes could only interact with other General Electric mainframes. One of ARPANET’s project goals was to create a heterogeneous and dispersed network capable of linking mainframes of diverse manufacture.

ARPANET was eventually expanded and renamed the Internet in 1984; by then, the Internet linked about one thousand corporate and academic hosts. Widespread use of the Internet began in earnest around 1993, and since then its growth has been exponential. Experts anticipate that the Internet will continue to grow at its present astronomical rate, and will become increasingly mobile and social.

Enter cloud computing. The Internet is expanding rapidly, and its users are increasingly diverse, sophisticated, and dispersed. Cloud computing is an efficient means to fulfilling users’ computing needs. The National Institute of Standards and Technology, defines cloud computing as “a model for enabling ubiquitous, 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.” Simply put, cloud computing enables consumers of IT services to offload IT expenses and obtain flexible computing services without having to rely on hardware in a specific location.
The cloud consists of five core characteristics (on demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), three service models (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)), and four deployment models (private cloud, community cloud, public cloud, and hybrid cloud). Entities choose certain service and deployment models based upon their individual needs and goals.

The benefits of cloud computing are legion. For businesses, cloud computing enables lower initial investment for new digital solutions, truncated deployment times, accounting recognition and improved cost control, strengthened service models, and it facilitates easy mobile access for employees. For the casual consumer, cloud computing makes email and other services available from multiple and varied devices.

B. The Cloud Darkens

For all of its benefits, cloud computing has some ponderous downsides. Because of its relative novelty, governance has yet to be developed, creating policy gaps; it is often unclear which law will be applied to fill these governance gaps. This state of affairs leads to uncertainty and unease in regards to what levels of protection individuals’ data can expect when in the cloud. It also remains unclear whose protections users are entitled to and which laws the data is subject to. These vexing problems are highlighted by an event that took place during the summer of 2011.

In a press conference occasioning the launch of Office 365 (Microsoft’s cloud service) the managing director of Microsoft UK, Gordon Frazer, was asked about the extent to which Microsoft could guarantee that the information of European citizens using Microsoft cloud services, stored in the EU, and held in EU data centers would be safe from the reaches of the USA PATRIOT Act. Frazer conceded that neither Microsoft, nor any other cloud services

36. MELLO & GRANCE, supra note 34, at 2–3.
38. Opinion of the European Economic and Social Committee on 'Cloud Computing in Europe,' 2012 O.J. (C 24) 40, 43 [hereinafter Opinion].
40. See Brad Smith, Gen. Counsel, Microsoft, Keynote Address at the Brookings Institution Symposium: Cloud Computing for Business and Society (Jan. 20, 2010), available at http://www.brookings.edu/~/media/Files/events/2010/0120_cloud_computing/20100120_cloud_computing.pdf (“We now need new action by Congress to modernize the protection of privacy and fill in these legal gaps.”).
41. Id.
42. Id.
44. Zack Whittaker, Microsoft Admits Patriot Act Can Access EU-Based Cloud Data, ZDNET (June 28,
provider incorporated or headquartered within the United States, could make such a guarantee to its European consumers in the event that information was requested under the Act. 45 Though data is generated, hosted, and accessed exclusively from the EU, data is not completely shielded from the long arm of U.S. law if the entity hosting the data has a U.S. presence. 46

Understandably, this revelation caused consternation within the EU. The notion that the information of European citizens saved and located within the EU could become subject to the intrusive laws of another nation simply by virtue of being contained in a cloud provided by a corporation of that country is intensely troubling, especially if laws are construed more conservatively or liberally in one country. Such thorny extraterritoriality 47 questions are engendered by the cloud s fundamental nature—it is a global and borderless technology. What is the justification for applying one nation s laws to another nation s data? More importantly, what is the principled approach for dealing with these issues as they arise?

Though the United States and the EU established a “Safe Harbor” agreement in 2000 48 permitting U.S. companies to transfer data from their EU subsidiaries to the United States subject to certain privacy restraints, 49 the passage of the USA PATRIOT Act in the wake of the 9/11 terrorist attacks altered the legal landscape and impacted the scope of the Safe Harbor agreement. 50 The Safe Harbor agreement established seven “privacy principles” aimed at protecting EU data from undue scrutiny. The principles as established were notice, choice, onward transfer (transfer to third parties),

45. Whittaker, supra note 44.
access, security, data integrity, and enforcement.\textsuperscript{51} Although firms opting into the Safe Harbor agreement are considered to be providing at a minimum “adequate” protections for the data of EU citizens,\textsuperscript{52} as U.S. law presently stands, requests made under the USA PATRIOT Act may effectively circumvent these privacy protections, allowing U.S. officials to reach data if they believe that the data is relevant to counter-terrorism measures.\textsuperscript{53} While the Safe Harbor principles call for disclosure and notice to citizens,\textsuperscript{54} information requested under the Act does not have to comply with these procedural values, thus vitiating the safe harbor provision.\textsuperscript{55} Nevertheless, in most other privacy contexts, the Safe Harbor provisions are still functional and are honored by both the United States and the EU.\textsuperscript{56}

C. A Wrinkle: Data Sovereignty?

As of now, data sovereignty is still a nebulous term.\textsuperscript{57} However, it is not without content. The issues arising from the challenges to the Safe Harbor agreement presented by the USA PATRIOT Act demonstrate that data sovereignty questions implicate more than just theoretical questions of law.\textsuperscript{58} Sovereignty is defined as supreme dominion, authority, or rule—the supreme political authority of an independent state.\textsuperscript{59} It is alternatively defined as the state itself.\textsuperscript{60} Sovereignty is further broken down into two categories: external sovereignty, which is the power of dealing on a nation’s behalf with other national governments, and internal sovereignty, which is the power that rulers exercise over their own subjects.\textsuperscript{61} Data sovereignty, or sovereignty in the context of cloud computing, is simply the notion that data should be subject to the laws of the nations in which it is created and stored.\textsuperscript{62} The notion that a

\begin{itemize}
\item 51. U.S.-EU Safe Harbor Overview, supra note 48.
\item 54. U.S.-EU Safe Harbor Overview, supra note 48.
\item 55. Whittaker, supra note 44. One of the cornerstones of the Safe Harbor agreement is that organizations must provide notice of disclosure to service users. See U.S.-EU Safe Harbor Overview, supra note 48. Nevertheless, as Gordon Frazier observed in the Office 365 launch press conference, U.S.-headquartered companies cannot guarantee that EU citizens would receive said notice if the U.S. government compels their data under the USA PATRIOT Act. Whittaker, supra note 44.
\item 56. See Constantin, supra note 53 (indicating that, outside the USA PATRIOT Act loophole, safe harbor provisions are honored by both the United States and the EU). See Zachary N. J. Peterson et al., A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud, 3 USENIX CONF. ON HOT TOPICS CLOUD COMPUTING 2 (2011), available at http://rbeverly.net/research/papers/soverign-hotcloud11.pdf (“[D]ata sovereignty has been recognized but not given a name by cloud practitioners . . . .”).
\item 57. See infra Part II.B.
\item 58. BLACK’S LAW DICTIONARY 1402 (7th ed. 1999).
\item 60. Id.
\item 61. Id.
\end{itemize}
private entity could, at the behest of another government, effectively abrogate this sovereignty in the cloud is a frightening one. However, overregulation of such a powerful but nascent technological resource is hardly a more desirable outcome. This issue must be dealt with in a balanced manner that protects citizens’ rights in the cloud while allowing the cloud to maintain the flexibility that is its foremost feature and will permit it to evolve and fulfill its potential without becoming stymied by over-regulation.

This is all the more important as the EU appears poised to introduce new regulations that will severely hamper the freedom to transact within the cloud for the sake of greater privacy of its citizens. While the importance of privacy can never be overstated, the EU’s approach to cloud computing is disproportionate to the risks inherent within the technology. Any legal framework purporting to police the cloud must be assiduous in refraining from excessive regulation and permit a space for the private sector to be innovative in developing approaches to cloud governance and the creation of flexible norms that will protect the world within the cloud.

The following part will provide a comparative analysis of the current state of U.S. and EU legal approaches to the challenging issues presented by cloud computing and will analyze the respective weaknesses and strengths of each. The part will also highlight the flaws inherent within an approach attempting an imposition of borders on the cloud’s reach while probing into some of the cultural socio-political factors underlying the divergent approaches towards cloud governance norms.

### III. ANALYSIS

Though the jurisdictional and privacy challenges posed by cloud computing are legion, the benefits of the technology are myriad. It drastically reduces operating costs of private business and government alike, greatly improves accessibility to and transmissibility of data, and creates an expanded and borderless world. Any regulation set forth to govern the cloud must be visionary, recognizing these unique features and making all efforts to construct governance frameworks that will not unduly constrain the cloud. When it comes to cloud regulation, the devil is truly in the details. How the regulations are effectuated is of the utmost importance, as the cloud’s growth potential should be preserved. For better or for worse, regulations enacted now will set

---

63. See Cooper, supra note 48. (“In particular, concerns have been voiced that recent legal developments, in particular passage of the USA Patriot Act, could fatally undermine a company’s Safe Harbor commitments.”).

64. Constantin, supra note 53.


the tone for the cloud’s future development.\(^\text{67}\)

**A. EU Response to the Cloud**

In a 2011 blog post on the European Commission’s website, Vice President of the European Commission Neelie Kroes posed a series of principles for the regulation of EU data located in clouds.\(^\text{68}\) First, Kroes proposed the establishment of a legal framework for “data protection, privacy, and . . . the allocation of jurisdiction . . . .”\(^\text{69}\) Second, Kroes proposed that the EU play a more central role in the standardization of Application Programming Interfaces and data formats.\(^\text{70}\) Kroes’ third principle was encouraging the public sector to take advantage of the benefits that cloud computing affords.\(^\text{71}\)

**B. Principled? Or Problematic?**

Kroes’ third principle is completely unobjectionable; indeed, it is laudable. The EU must take advantage of the cloud’s power. The U.S. government has already transitioned into the cloud, enabling it to leverage shared infrastructure and economies of scale.\(^\text{72}\) It also has resulted in the reduction of infrastructure and usage costs.\(^\text{73}\) The governments of the member states of the EU would undoubtedly benefit from making a similar shift, especially in the face of crushing budget shortfalls.\(^\text{74}\) However, elements of Kroes’ first and second principles are cause for alarm.

Kroes’ call for government-centered data standardization and jurisdictional allocation should not be taken lightly and should be called what it is: an unwarranted attempt to involve government in the business of limiting how citizens interact in the cloud, dictating where these transactions can take place, and dictating where the proof of these transactions can be stored. It is an attempt to control a market that can and should be self-regulating.\(^\text{75}\) Indeed,
even the notion that there exists an unequivocally “clear role” for public authorities to assume in the realm of cloud computing is in itself problematic. This notion is an overly simplistic and reductionist view of the complexities specific to cloud computing and of the impact of government regulation on technological development more generally. There is no clear role for any one entity to assume in this arena. There is, however, nuanced interplay between public policy and private development.

Requiring that data centers be located in specific countries is a limited, and indeed, undesirable remedy for two reasons: one that relates to the philosophical underpinnings of the cloud, and a second that relates to the realities of inadvertence and human error. Firstly, regulations that come in the form of limitations on where cloud data can be stored, for example, would destroy one of the main features of the cloud—its borderlessness.

“Borderlessness” is not simply meaningless philosophical musing. This matters because borderless applications endow the cloud with its characteristic infiniteness and flexibility. This same trait “enable[s] Internet technologies to provide higher quality, [more] agile solutions” via the cloud. Borderlessness can be converted into the tangible—into dollars and cents. For entities utilizing cloud services, it provides them with greater return on investment by enabling business to “build only what is core to their business,” instead of using service packages containing extraneous and inutile products.

Placing legal restrictions on the location of data centers could destroy cloud computing’s borderlessness and cost effectiveness by creating situations wherein cloud services users are effectively barred from bringing their business to the cloud service providers offering the precise service packages they demand. Instead, users will be forced to utilize the services of cloud providers storing data in specific (and presumably government-approved) locales. This would occur notwithstanding the fact that these providers may not necessarily be capable of providing the precise service packages sought. Needless to say, the practical effect of such regulations will also be an increase in overall service costs. What cloud services users are left with, then, are

---

76. See, e.g., Kroes, supra note 68 (arguing that there is a clear role for the EU to play in instituting cloud computing reforms).
77. See Peterson et al., supra note 57, at 1 (noting the complexities of agreements requiring that data centers be located in particular locations and arguing that “a suite of existing and future tools” will be needed to address these concerns).
80. Id.
82. Id.
83. Id.
increased prices and diminished flexibility.

Secondly, this approach would not provide protections against inadvertent transfers or leaks of data. In the cloud context, form has a direct impact on function. That is to say, artificially attempting to constrain the boundaries of the cloud would strip it of the very properties from which it derives its power. Placing legal limitations upon the physical locations of data centers powering the cloud and containing user data will not lead to greater security in the cloud if adequate technological measures to ensure that the cloud itself is secure are lacking and “best practices” for data protection within the cloud are not articulated.

Practically speaking, current legal and jurisdictional frameworks are heavily rooted in anachronistic traditions, ones that evolved ages before the advent of mass electronic communications. These jurisdictional frameworks employed methods of determining applicable law, as well as the rights and duties of actors based upon where the actors themselves were located (in personam jurisdiction) or where the actors’ property was located (in rem jurisdiction).

However, jurisdictional methods based on locations, physical borders, and tangible entities are unsuitable for a technology like cloud computing, which derives its power in large part from its ability to transcend borders and connect billions of users all across the globe—all citizens of different states. Attempting to mandate that data be maintained on servers housed in certain locales will vastly reduce the cloud’s seamlessness, its ability to transmit data to whomever wherever they may be located with ease. Such a move would essentially reduce the cloud’s reach, constraining it to a few servers located in

(1975) ("These estimates . . . suggest that the total costs of regulation may be extremely high, given that about 17% of GNP originates in industries—such as agriculture, transportation, communications, power, banking, insurance, and medical services . . . . Indeed, the costs of regulation probably exceed the costs of private monopoly." (emphasis added)).

85. Peterson et al., supra note 57, at 1.

86. An architectural philosophy espoused by architect Louis Sullivan (1856–1924), “form follows function,” is the notion that the shape of a building or object should be primarily based upon its intended function or purpose. Carl W. Condit, Sullivan’s Skyscrapers as the Expression of Nineteenth Century Technology, 1 TECH. & CULTURE 78, 79 (1959). This notion has direct application to cloud computing infrastructure. As the cloud is intended to be flexible and global, regulations that constrain the cloud’s scope, by imposing legal limitations on the physical locations of the data centers powering the cloud, will impact the cloud’s utility by inhibiting its reach.


91. Seamless Cloud Computing (SeCCo), PURDUE U., http://www.cs.purdue.edu/homes/peugster/SeCCo/ (last visited Apr. 12, 2013) (“Seamless cloud computing (SeCCo) aims at smoothening the boundaries to and between computing clouds.”).
designated “safe house” countries.\textsuperscript{92}

Furthermore, while data security is a legitimate concern in the arena of cloud computing, mandatory geolocation of data centers, \textit{(i.e.,} governments predetermining where the cloud servers that service their citizens’ data may be located\textit{)} does nothing more than to provide a false sense of security while failing to render the cloud \textit{itself} any more secure in a global sense. Such a move would do nothing to prevent data from accidentally or inadvertently being transferred from approved “secure” locations to ones deemed less secure. Protections from these potential threats are best provided by improving encryption technologies. This would strike the necessary balance between security and the maintenance of the cloud’s fundamental utility.

This heightened level of security is not necessarily achieved by increased government regulation imposing jurisdictional limitations, but rather will be the result of such measures as increased research into and development of improved encryption technology\textsuperscript{93} and bold experimentation with new models of data storage that increase data security while simultaneously decreasing the need for heavy reliance on the integrity of service providers.\textsuperscript{94}

Furthermore, EU restrictions have already been limiting the growth of cloud computing in Europe.\textsuperscript{95} Europe lags behind the United States in the development of cloud technologies, and the severe restrictions imposed on the cloud have had the effect of slowing the cloud’s evolutionary trajectory in Europe.\textsuperscript{96} It appears that liberalization, rather than intensified regulation, is what Europe needs if it wants to truly unleash the cloud’s power. A less heavy-handed approach is crucial for the technology’s future in the EU.

\textbf{C. The U.S. Response to the Cloud}

The U.S. approach to the cloud has been markedly different from the EU’s approach to dealing with cloud conundrums. In December 2010, the federal government transitioned to a “Cloud First” policy aimed at “using cloud technologies where feasible.”\textsuperscript{97} Entities at the state and local levels of

\begin{itemize}
  \item \textsuperscript{92} See \textit{Id.} (“\[E\]xisting support is geared towards vanilla setups where everything is colocated in a single datacenter, which contradicts many existing and emerging real-world scenarios. Bringing all data to the ‘mothership’ prior to executing an analysis task is tedious at best and in most cases exhibits poor performance.”).
  
  \item \textsuperscript{93} \textit{What Is Homomorphic Encryption?}, \textsc{wise}GEEK, \textsc{http://www.wisegeek.com/what-is-homomorphic-encryption.htm} (last visited Mar. 5, 2013) (“With the advent and continual expansion of cloud computing, coming up with a viable homomorphic encryption method is crucial. Otherwise, the risk is too high to entrust data to a cloud-computing provider when those data must remain secure.”).
  
  \item \textsuperscript{94} Jennifer L. Schenker, \textit{Cloud Computing W\textendash}with Borders May Be on Horizon in Europe}, \textsc{INFORMILO} (May 18, 2010), \textsc{http://www.informilo.com/20100518/cloud-computing-borders-may-be-horizon-europe-276}.
  
  
\end{itemize}
U.S. government have also embraced cloud computing, and the American private sector has been using various forms of cloud computing technology for some time. In the face of cloud computing’s ubiquity and novelty, some within the computing community have even exhorted Congress to adopt a laissez-faire approach to regulation of the technology, at least for the time being.

Notably, President Obama recently responded to threats posed to privacy and security by cloud computing not with a “call to arms” for stricter regulation of the computing industry, but instead with a call for the expansion of privacy laws in order to ensure liberty in the cloud. This divergence is likely attributable to several causes. Firstly, most of the major cloud providers are American corporations providing services to American consumers who have had ample time to become accustomed to cloud computing, notwithstanding reservations that they may have concerning possible security risks.

In addition, U.S. law already has extant legal frameworks that do an adequate job of protecting web users from fraud and other computer- or data-related malfaiseance. One of the primary protections comes in the form of the Computer Fraud and Abuse Act (CFAA). The CFAA’s basic provisions bear fines and criminal penalties for individuals or entities intentionally interfering with computers in order to damage or impair them, unlawful accessing of data, and use of computer devices to effect fraudulent transactions.

With seven categories of cybercrimes (transmission/acquisition of national security information, intentionally gaining unauthorized access to a computer, trespassing in a non-public government computer, using unauthorized access to defraud or gain access to something of value, gaining...
unauthorized access and causing damage to a computer,\textsuperscript{110} trafficking in passwords,\textsuperscript{111} and threatening to cause damage to a computer with the intent to extort\textsuperscript{112}), it is currently the best line of defense that the United States has to combat crimes in and against data in the cloud, though some argue that the CFAA, an electronic communications act promulgated in 1986, is outdated and completely incapable of handling a brave new world of cloud computing.\textsuperscript{113}

Though punitive legal measures do exist as enforcement mechanisms to deter against cloud criminals, the CFAA is entirely retrospective and is lacking in provisions that will prevent criminals from successfully accessing data in the first place.\textsuperscript{114} However, this is a state of affairs that only the private sector can solve by developing improved security measures for cloud consumer data and ensuring that all data centers are reasonably secure before contracting for services.\textsuperscript{115} These are protections that will be developed, offered, and driven by consumer demand rather than government regulation.

There are several other existing tools in the United States’ cloud computing security arsenal, namely a series of sector-specific legislation governing privacy.\textsuperscript{116} Among these regulations are the Gramm-Leach-Bliley Act\textsuperscript{117} and the Fair Credit Reporting Act\textsuperscript{118} for the financial services sector and the Health Insurance Portability and Accountability Act for the health care sector.\textsuperscript{119} In addition, the Payment Card Industry Security Standards exist as non-governmental, self-regulatory best practices for the credit and debit card industry.\textsuperscript{120} The function of these laws is to protect consumer information by requiring that service providers within each sector adhere to certain disclosure and privacy laws when client information is provided to third parties.\textsuperscript{121} Obviously, in the cloud context, these same confidentiality and security

\begin{itemize}
\item \textsuperscript{110} Id. § 1030(a)(5)(A).
\item \textsuperscript{111} Id. § 1030(a)(6).
\item \textsuperscript{112} Id. § 1030(a)(7).
\item \textsuperscript{113} See Smith, supra note 40 (noting that the CFAA must be “modernize[d]”).
\item \textsuperscript{114} See 18 U.S.C. §§ 1028A–1030. The statute as promulgated was designed to punish cyber criminals ex post, after the commission of a crime. However, the law is powerless to prevent criminals from accessing data on computers or in clouds. This is generally a limitation of legislation—it can punish but not always prevent.
\item \textsuperscript{115} See Microsoft Speaks Out, supra note 87 (explaining that private cloud computing vendors may be able to provide higher levels of security).
\item \textsuperscript{118} Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2006).
\item \textsuperscript{120} See generally PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES, VERSION 2.0 (2010), available at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.
\item \textsuperscript{121} RUIJTER & WARNER, supra note 116, at 13–16.
\end{itemize}
requirements still apply. According to the law, service providers must still guarantee the same disclosures and protections.

A secondary benefit of these sector-specific measures is that they provide a framework for self-regulatory measures within industries without discouraging self-regulation in other industries. This is beneficial, as it provides layers of protections for users within the cloud—the federal regulations that providers must be in compliance with and the self-regulatory norms and measures that service providers can institute within the cloud.

Protections in the cloud are more comprehensive than detractors intimate.

D. Why the Divergence?

There is a clear schism developing here. European and American responses to the growth of cloud computing have been markedly different. Many European and American regulatory policies remain highly divergent. In order to thoroughly analyze the issue, it is necessary to explore the precise root causes of the differing attitudes. Partly sociological and partly political, the differing approaches to the regulation of this new technology implicate old policy questions concerning the proper role of government versus the primacy of the private sector.

Respective European and American views concerning these questions play out in this newest debate. Some suggest that the two governments’ understandings of the need to manage, legislate, and regulate risk impact the ways in which the two political entities approach technology regulation. The literature emerging from both the United States and the EU lends credence to this assertion. Much of the EU material regarding cloud computing highlights its concerns about information and power asymmetries—that users do not fully comprehend the nature of the technology that they are consuming and cannot adequately negotiate rights and duties at the service level.

In the EU, there is much hand-wringing about what “supervisory

122. See id. at 12–14 (discussing the privacy standards applicable to cloud computing service providers).
123. Id. at 10–14.
124. Id. at 5.
125. See id. (discussing sector-specific laws as a backup for failures of self-regulation).
126. See supra Parts III.A, III.B, and III.C.
130. VOGEL, supra note 127, at 5.
131. Opinion, supra note 38, at 40.
132. Id. at 41.
authority” will emerge to deal with dispute resolution and compliance. Others point to such political phenomena as the presence of powerful lobbies and interest groups pressing either protectionist or free-market preferences to the government—with European technology lobbies leaning towards protectionism and American lobbies expressing preferences for more laissez-faire, free-market governance models.

As it relates to the cloud, the difference between the U.S. and Europe is the difference between reactivity and proactivity. The U.S. seems to be content to permit the technology to develop and expand, while addressing concerns as they arise and as the contours of the cloud become more defined. The European approach is to manage the technology based on what is currently known about it to prevent theoretical problems and abuses from ever arising. The conversation in Europe is best characterized as one centered on finding ways to diminish the cloud’s breadth for ease of control and management, rather than embracing the cloud’s expansiveness and finding ways to work through its quirks in order to preserve its great utility.

E. Importance?

There is an important distinction to be made between regulation of the cloud itself and regulations of rights and duties of parties transacting within the cloud. The European approach is one of direct regulation of the cloud, while the American approach is one centered on a regime that focuses on rights and duties in the cloud context. Direct regulation of the cloud (i.e., measures mandating jurisdictional limits on the cloud databases—cloud protectionism) should be avoided to the extent feasible because such regulations will inevitably restrain the growth of this technology, a technology with possibly unlimited potential. Apportioning rights and duties, however, will have the dual beneficial effects of preserving/elucidating the rights of individuals within the cloud while leaving the cloud unencumbered and able to realize its potential.

133. Id. at 46.
134. See, e.g., SWINNEN & VANDENMOORTEL, supra note 128, at 4 (discussing European protectionist lobbies in the context of biotechnology regulation).
135. See id. at 31 (discussing the United States allowing certain biotechnology and supporting it).
138. Id.
140. See Pop, supra note 66 (reporting how some have suggested the EU should not over-regulate cloud computing to avoid stifling its potential).
141. See id. (discussing how to ensure privacy for citizens while promoting development of the cloud).
Though the groundwork necessary to firmly establish rights and duties within the cloud is difficult, it must be done sooner rather than later. Cloud computing is a rapidly-growing technology of increasing relevance—the stakes are high. Much about cloud computing remains shockingly nebulous: questions regarding such issues as “the status of privacy and confidentiality in the cloud [remain] legally uncertain.” This uncertainty can be solved, however, by a cloud computing strategy emphasizing four crucial goals that will be discussed and elaborated upon in the following part.

IV. RECOMMENDATION

An effective, comprehensive cloud computing strategy should ideally consist of four primary goals: (1) keeping direct governance and regulation of the cloud to a minimum; (2) using and strengthening existing legal frameworks as a backdrop for the policing of the cloud; (3) permitting private actors to create norms and customs to police the cloud, especially through the use of tort and contract theories of liability; and (4) avoidance of enacting legislation that would have the effect of mandating that data centers be located in specific geographic locations.

A. Minimizing Direct Cloud Governance

The cloud’s appeal is its flexibility. Using the government as a source of norms in the early stage of the technology’s development will not only moot this flexibility, but will also have the effect of locking the technology in at its current state. A government-centric regulatory model in cloud computing is inadvisable, as government is not sufficiently responsive to keep pace with the rapid manner in which technology evolves. Consumers will be the ones to shoulder the burdens of the cost of regulations made in ignorance of the technology’s full potential.

This Note is primarily intended to be a comparative exploration of regulatory norms and a survey of the present state of technology law as it relates to cloud computing. Resolving the complex data sovereignty issues that exist is a complicated proposition that realistically may involve treaties, agreements, and a great deal of international cooperation—no small feat. However, if a state of affairs wherein cloud providers are permitted to use the global free market and store data in centers located in various parts of the world without onerous government restrictions is seen as a necessary and

144. Id.
145. Robert W. Hahn & Anne Layne-Farrar, Is More Regulation Needed to Promote e-Commerce?, 35 CONN. L. REV. 195, 213 (2002) (“There is a very real danger that federal regulation of a market that is changing rapidly...could impose net costs on consumers.”).
146. Smith, supra note 40.
desirable good, governments will have to coordinate efforts to avoid treading on toes due to extraterritorial overreach.147

Though there are many who believe that governmental regulation of all aspects of cloud computing is the only way to achieve optimal results as it relates to privacy, security, and data protection,148 the ideal and considered approach to the question of cloud governance would be to permit governments to regulate in limited contexts (i.e., jurisdictional issues) while permitting private actors to create codes of conduct, norms, and best practices.149

B. Utilization and Strengthening of Existing Statutory Frameworks

Enhanced national privacy legislation may be necessary to protect citizens in both the United States and the EU, but government regulation should not exceed these measures. Present U.S. legislation—e.g., the CFAA, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, etc.—should be improved and language that reflects recent changes in technology should be added to the legislation in order to provide greater protections for cloud services consumers.

For example, one valid criticism of the CFAA is that its conception of computer fraud and computer breach is an archaic one, one centered on hacking into an individual personal computer (PC).150 Currently, the CFAA levies the same penalties against an individual hacking into an individual computer and an individual hacking into a data center.151 Given the diffuse nature of the cloud, an unauthorized data center breach could cause substantially more damage than an individual PC breach.152 Presently under the CFAA, however, a data center hacker would not be made liable for the full scale of the damage caused—the liability imposed would not properly reflect the extent of the actual damage caused.153

The solution to this shortcoming is to modernize the CFAA’s language so that it fully reflects the realities of modern cybercrime in the context of the new dispersed networks that are used. It simply needs more teeth: the criminal and civil penalties must be stiffened and increased, data center hacking must be addressed within the context of the CFAA, punishments must be afforded in proportion to the scale of the crime, and the CFAA itself should be strengthened and made more technology-neutral so as to prevent its obsolescence in the future.154

147. See Himelfarb, supra note 47 (describing the problems associated with extraterritoriality).
148. Smith, supra note 40.
150. Smith, supra note 40.
151. Id.
152. Id.
153. Id.
There are some who view the CFAA and other cybercrime legislation of its ilk as being fatally outdated, and advocate for a corps of completely new cloud-specific legislation to police the cloud in addition to the modernization of existing legislation. However, for all its well-meaning concerns, this view only provides a limited solution. As a nouveau technology, the depth and breadth of its potential is largely an unknown. For any government to attempt to legislate into an informational void without having a full grasp of what is at stake would be a problematic proposition. Instead, legislators in both the United States and the EU should be as legislatively conservative as possible, amending legislation as threats arise (and as more complete information becomes available) rather than taking preemptive strikes that might have unintended negative impacts on the technology’s growth and might increase the cost of cloud services.

C. Policing the Cloud Through Private Norms and Customs

The most important aspect of this recommendation however, is that private actors be able to create norms for policing regimes for the cloud. Many cloud computing relationships are already dealt with contractually and cloud consumers are able to use contracts to define the contours of the vendor–consumer relationship: functionality, termination, price caps, and privacy are generally issues that are negotiated around when the parties sit down to contract. It would also be feasible for cloud users to use tiered services, with differing levels of security permitting the consumers to opt in and out to provide themselves with greater security depending upon the sensitivity of the data stored within the cloud.

Cloud users and providers could also include contract terms that will streamline the resolution process in the event of a contract breach. Basically, parties could include remedies within the four corners of the contract. For example, remedies such as liquidated damages clauses could be included in contracts for cloud computing services. Furthermore, users and providers can use other traditional dispute resolution approaches to resolve conflicts (e.g., mediation, binding arbitration, agreeing beforehand to forum selection clauses) within the computing services contract that dictate which state or

155. See Smith, supra note 40 (“We need Congress to modernize the laws, adapt them to the cloud, and adopt new measures to protect privacy and promote security.”).

156. Id.

157. See Hahn & Layne-Farrar, supra note 145, at 213 (“There is a very real danger that federal regulation of a market that is changing rapidly, such as e-commerce, could impose net costs on consumers.”); see also Posner, supra note 84, at 818 (“[T]he total costs of regulation may be extremely high . . . .”).


160. Forum selection clauses are an effective way to resolve jurisdictional issues by determining beforehand which law will apply in the event of a contract dispute. See, e.g., Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585, 595 (1991) (upholding forum selection clause contained within a form ticket contract); see also RESTATEMENT (SECOND) OF CONTRACTS § 345 (1981) (noting other judicial remedies available to protect a party’s interests).
nation’s laws will apply in the settlement of a contract dispute, should one arise. Should norms within the cloud fail, users and providers clearly have effective recourse even in the absence of legislative intervention.

In addition, tort law would always be available as recourse against cloud computing services intentionally or negligently compromising privacy or sensitive information. As cloud services provider Dropbox has learned, aggrieved customers whose information in the cloud has been negligently compromised will use the tort system to seek damages for loss resultant thereof.

In the event of an intentional data leak, or if a cloud provider intentionally provides a user’s information to a third party without the user’s permission or consent, it seems obvious that users could sue the services provider in tort (presumably under trespass to chattel or some similar theory) and not only obtain compensatory damages but punitive damages as well, if a jury deems the provider’s conduct to be particularly flagrant. An award of punitive damages could signify substantial and ruinous liability for cloud services-providers that intentionally compromise user data contained in their clouds. Though some schools of thought view this possibility as a harm rather than a good (or at the very least, do not believe that punitive damages always accomplish their stated deterrent ends), the reality is that the specter of punitive damages is often powerful enough to discourage blatant and intentional misbehavior on the part of cloud services providers.

Furthermore, harmed users could also feasibly obtain injunctive relief when appropriate to prevent the cloud services provider from continuing to compromise their information in the event of ongoing tortious behavior. In the event of a merely negligent breach, where a harmed user successfully demonstrates that the four necessary elements of negligence are present, that


163. Restatement (Second) of Torts §§ 903, 908 (1979) (defining compensatory and punitive damages).


165. See generally John Calvin Jeffries, Jr., A Comment on the Constitutionality of Punitive Damages, 72 VA. L. REV. 139 (1986) (questioning the constitutionality of punitive damage awards); A. Mitchell Polinsky & Steven Shavell, Punitive Damages: An Economic Analysis, 111 HARV. L. REV. 869, 875–76 (1998) (arguing that punitive damages against a corporation may not have the intended effect).

166. See Clarence Morris, Punitive Damages in Tort Cases, 44 HARV. L. REV. 1173, 1207 (1931) (noting that the threat of punitive damages may deter potential wrongdoers); see also Harvey R. Levine, Demonstrating and Preserving the Deterrent Effect of Punitive Damages in Insurance Bad Faith Actions, 13 U.S.F. L. REV. 613, 627 (1979) (“The most desirable characteristic of the punitive damages verdict is its admonitory function . . .”)

167. See Restatement (Second) of Torts §§ 933, 936 (1979) (enumerating factors in determining appropriateness of injunctive relief).
user would be able to recover compensatory damages as well.\footnote{168}{See id. § 903 ("‘Compensatory damages’ are the damages awarded to a person as compensation . . . for harm sustained by him.").}

Without a doubt, use of such common law measures of cloud policing should be encouraged because such suits will indemnify injured users and will also have the effect of fostering competition. Cloud providers will compete to develop comprehensive services that provide reliable levels of protections and stronger warranties against breach in order to defend against the prospect of crushing liability.\footnote{169}{See Tim Cowen, \textit{Competition Law Issues in Cloud Computing}, SCL (Oct. 2, 2013), http://www.scl.org/site.aspx?id=30526 ("When dependence can be shown to arise because of the dominance of a supplier, it can be addressed under competition law.").}

All in all, it seems safe to assert that the private sector is equipped to handle the multifarious legal questions arising from the increasing use of the technology and can continue to deal with the concerns without heavy-handedness on the part of governments, European or American. Indeed, Google’s response to the recent hacking attempts made in China illustrate that industry is prepared to respond aggressively to threats posed to the cloud.\footnote{170}{See Obaiduzzaman Khan, \textit{Google Chrome Will Encrypt Gmail}, TSC J. (June 16, 2011), http://thetechjournal.com/internet/web-security/google-chrome-will-encrypt-gmail.xhtml (discussing Google’s approach to security after Chinese cloud hacking); see also Michael Joseph Gross, \textit{Enter the Cyber-Dragon}, \textit{Vanity Fair}, Sept. 2011, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109 (discussing Chinese security breach attempts).}

Interestingly, earlier EU technology directives advocated a contractual approach towards the regulation of emergent technologies.\footnote{171}{See generally Council Directive 2009/136, art. 20, 2009 O.J. (L 337) 11, 13 (EU).} The previous iterations of EU policy dealing with technology regulation and the processing and maintenance of user data advocated for wider use of contract to police user–provider relationships.\footnote{172}{Id.} There is nothing to suggest that similar approaches to cloud computing could not be adopted. Indeed, the EU would stand to benefit from a return to more liberal, consumer-centric technology policies.

\textbf{D. No Mandated Geolocation of Cloud Data and Data Centers}

A linchpin of the proposed cloud regulations is mandating that cloud data be stored exclusively on data servers in specific geographic locations deemed to be more secure.\footnote{173}{See Peterson et al., \textit{supra} note 57, at 1 ("Of particular interest is establishing data location at a granularity sufficient for placing it within the borders of a particular nation-state.").} The EU has already indicated its preference that servers should be located on EU soil to preserve data sovereignty and to ensure that its laws will be applied to citizens’ data.\footnote{174}{Microsoft Speaks Out, \textit{supra} note 87 (mentioning that new Australian data sovereignty legislation was modeled after similar EU legislation designed to keep data from leaving the region).} However, this is a solution that does not answer the more fundamental and separate question of \textit{how to best keep data secure}. Whether this measure will accomplish the EU’s data security prerogatives remains to be seen. Though the EU may succeed in blocking the offshoring of data servers, this alone will not ensure that sensitive data is kept...
secure in the first place. The EU’s proposed regulations will do nothing to solve the cross-border data flow issues and the definitional gaps that exist under the present regime. Worse still is the possibility that these EU regulations may further hamper the cloud’s growth, in a trade-off between data security and functionality.

As Microsoft noted in response to a draft data sovereignty bill: “[b]y regulating the geography where the data is held rather than the level of security under which it is held[, the legislation] implicitly establishes criteria for data protection that are not related to principles of technology security.” The principal problems with the EU’s approach to data sovereignty is that it stifles the competition necessary to develop truly secure data centers and potentially leaves user information susceptible to breach in minimally secure, albeit onshore locations. Rather than mandating and regulating the geographic location of data centers powering the cloud, the better solution would be to invest in the private technology sector and to encourage the sort of innovation that will improve encryption techniques and will make data centers less susceptible to breach, leaks, and attacks. There is no reason to believe that the private sector is ill-equipped to undertake these various challenges within cloud computing.

V. CONCLUSION

Cloud computing is not without its risks. In the early stages of any new technology, there are innumerable hazards and unknowns. The proper response is to establish a set of guiding norms while strengthening existing ones, rather than attempting to regulate variables and unknowns before an actual threat is even identified. Cloud computing’s potential cannot be overstated. It is a potent technology that connects individuals, renders communication infinitely simpler, and streamlines the operations of business and government while reducing costs.

Cloud computing is efficient; cloud computing is new. Regimes for policing it that we develop now from behind our veil of ignorance—unaware of what it will become—will set the tone for its future; any missteps made during this phase of its evolution might result in foreclosing opportunities for its growth and development.

The future of cloud computing depends upon the ability of actors within the cloud to independently construct a legal infrastructure that can adequately police while respecting the unique aspects of the cloud (i.e., the borderlessness

175. Id.
177. Id.
178. Microsoft Speaks Out, supra note 87.
179. See id. (“[Australian data sovereignty legislation] actually prevents the Australian e-health records [from] being kept in the most secure data centres abroad.”).
180. See Nelson, supra note 67, at 76 (“Governments can add value by encouraging experimentation and new services.”).
and flexibility) that render it as revolutionary as it is. This can be most effectively accomplished by permitting private entities to have a central role in cloud governance: allowing service providers to make the decisions regarding how they will provide services while allowing users to freely make the decisions regarding the types of cloud services that they will utilize and the level of risk that they are willing to assume, without paternalistic hand-holding.

In the early days of any new technology, it always appears unwieldy and ungovernable—the collective first impulse is often to legislate first and ask questions after. However, in this case, it would be dangerous to yield to this impulse so early in the game, especially without a complete knowledge of the technology’s dimensions or potential. Legislative schema for cloud computing may very well freeze the technology in its present state and destroy value for consumers.

Legislative temperance is the best approach for the time being, allowing actors within the cloud to remain autonomous and innovative in the development of independent norms and customs that will be malleable enough to accommodate the cloud’s flexibility while authoritative enough to ward off the darker clouds of insecurity and lawlessness that may gather within the world of the cloud. This as a goal is not impossible, but simply ambitious. But then again, cloud computing is nothing if not ambitious.