“Every Cloud Has a Silver Lining, or Does It?”

VINCENT M. CATANZARO
Senior Counsel, Global Discovery Manager
E. I. du Pont de Nemours and Company, USA

&

KARINE TATOYAN
Member of the Pennsylvania Bar, USA

I. INTRODUCTION
Advertisements scream promises of unlimited resources and limited cost; a veritable pot of gold at the end of a rainbow. Providers tout a perfect cloud solution that can handle any problem of size and cost and eliminate the need to ever purchase a server again. Cloud computing can allow the buyer access to their information anywhere, anytime, on any device with the click of a button. All of this for a very low - very predictable - monthly fee that is a fraction of Information Technology (IT) costs. These clouds, however, may not be lined with silver, but rather, could prove truly hazardous for those who accept the environment without truly understanding what it is.

Cloud computing has become a phenomenon in the IT arena over the past few years as corporate users try to navigate the traditional model of in-house resources and the capitol costs of maintaining infrastructure, hardware and support staff. In its basic concept, cloud computing sounds enticing; let a technology expert handle the day-to-day maintenance of server output and storage while the user just reaps the benefits of that service, essentially outsourcing the IT function.

So how can they do it? How are these services available from cloud providers at such unbelievable prices? What did they figure out that the corporate world could not? The answer is twofold: scalability and location. A cloud provider can put all of its information in as few boxes as necessary and maximize storage space. Utilizing the ability to put information wherever they want, without regard for boundaries and physical access, providers take advantage of low-cost services. What may not be obvious about this arrangement is that the user has little to no control in deciding where their information is stored, what methods are used to secure their information, and whose information could be sitting right next to theirs in the cloud.

Cloud users need to be cognizant not only of the benefits of this technology but also the potential pitfalls and concerns they should have. What might be satisfactory for a personal user or small regional firm in respect to security, might not work for a multinational company with regulations and requirements that govern data security. This article will discuss the realities of cloud computing and the ways in which consumers can protect their interests as well as those of their customers. In a global world where cloud providers take advantage of all the resources available to them, users should also be aware of the restrictions and risks that these varied jurisdictions present.
II. WHAT’S AT STAKE
Recent predictions estimate that the global revenue for cloud computing services could reach $35.6 billion in the year 2013.¹ These figures present overwhelming proof of the potential impact that cloud services could have on the global economy. Considering the limited numbers of providers that currently dominate the cloud market, a failure by one can cause insurmountable damage and loss to the users of that service. The International Working Group on Cloud Computing Resiliency has estimated that Google, Microsoft and Amazon, which rank amongst the top providers of cloud services, cost nearly $200,000 to its customers for an hour of service outage.² An outage could mean more than just a temporary loss of usability, but could also result in a permanent loss of stored data.

For example, in 2011, Amazon’s Elastic Cloud Compute (EC2) service was unavailable to customers in the eastern United States for several days. Despite Amazon’s attempt to restore all of the data, reports indicated that the failure caused some customers to permanently lose their information.³ Similarly, in March of 2013, Microsoft’s Hotmail, Outlook.com and SkyDrive services, which are used by customers worldwide, were unavailable for almost an entire day.⁴ Such prolonged disturbances could cause a stoppage of business output for users who utilize Microsoft’s services to access e-mails and stored documents, which are essential functions to effective business operation.

Although these examples provide insight into the possibility of loss as a result of a system outage, most users of cloud services must also be aware of the potential for loss, resulting from data breaches. The Online Trust Alliance (OTA) reviewed 1,470 incidents of data breaches worldwide, recorded by the Open Security Foundation in 2012, and found that the security failures exposed more than 242 million records to intruders.⁵ The OTA concluded that over 97% of these breaches could have been prevented with the appropriate application of internal and external security measures.⁶

When standard security measures are not executed, who bears the burden of restoring the damage and recovering the loss? To properly address this question, one must first understand the infrastructure of the cloud and the various legal and regulatory provisions that affect its operation. With this requisite knowledge, users can adequately prepare to implement preventive procedures that safeguard stored information and provide a remedy to subsidize potential loss.

III. WHAT IS THE CLOUD?
The cloud began as an undefined drawing in a diagram outlining a corporation’s network. In an illustration to showcase the flow of data from the internal network to an external receiver, a drawing of a cloud separated the two ends to identify the route of traffic. It was a space that stored outgoing data before transmitting it to the end user. As far as “cloud computing,” there is much debate as to the origin of the term. Some claim an early 1990’s introduction, while others attribute much of its acclaim to Eric Schmidt of

---

⁶ Id.
Google, who used the term in a 2006 conference. The debates surrounding the origin of the cloud parallel the uncertainty of the technology. Many definitions have surfaced that have attempted to clear the mist. Despite any ambiguities, however, it is important to understand the inconsistencies in technology in order to best use the benefits while preparing for the risks.

As an example of the divergence in explaining the cloud, the following are some of the accepted definitions. Forrester Research defined the cloud as “a standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way.” The National Institute of Standards and Technology (NIST) defined the cloud as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” The U.C. Berkeley Reliable Adaptive Distributed Systems Laboratory (RAD Lab) gave a more elaborate definition, but also added that cloud computing was a service offered to the public that did not include private services offered to an organization that were not accessible by the public.

These examples fall on a spectrum of services that are combined to formulate the different definitions for the cloud. From a macro perspective, taking the similarities of the various descriptions, the cloud can be understood as a placeholder for data accessed by users, utilizing prescribed software. From a micro perspective, there are variations in the accessibility, locality, security and reliability of the software.

Generally, cloud computing has been categorized into three sectors: (1) Software-as-a-Service (SaaS); (2) Platform-as-a-Service (PaaS); and (3) Infrastructure-as-a-Service (IaaS). A Software-as-a-Service is a well-known method of cloud computing, where software is provided to the end user directly over the Internet (e.g., Salesforce CRM). A Platform-as-a-Service provides a development platform where the customer can use the service to develop, test, and deploy applications that are then hosted on the provider’s infrastructure (e.g. Google App Engine and Microsoft Windows Azure). Finally, an Infrastructure-as-a-Service is the simplest method that provides computing power, data storage, and other types of infrastructure to the end user (e.g. Amazon EC2, GoGrid, and Mosso). Each is an attractive option for most businesses because it alleviates the need for the use of additional IT resources as the providers manage the platform and infrastructure of the software externally.

Within each method, four different cloud deployment models have been identified by the NIST: the Public Cloud, Private Cloud, Community Cloud, and the Hybrid Cloud. The “Public Cloud” is an infrastructure owned by a service provider and made available

---

9 Id. at 9.
10 Id. at 10.
11 Id. at 16.
12 Iyoob, Ilyas Rossetti, Manuel D. Chen, Yaohua, Cloud Computing Clarity, Industrial Engineer: IE 45, no. 4, 32 at 34, April 2013.
13 Id.
14 Id.
to the general public.\textsuperscript{16} Most public clouds are free or offered on a pay-per-use basis. Although the most cost effective alternative, it also bears the most risk. With the increased accessibility, a public cloud provides more opportunities for security breaches, data loss, and service interruptions. The heightened security concerns also highlight problems with control and possession of the stored information. If the operating units of the infrastructure suffer damage, it can result in immeasurable loss to its users. When storing data on an external network, users risk this total loss of information, by entrusting the service provider with the management and security of the data. Due to these potential system threats, most organizations benefit from a more secure cloud model.

The “Private Cloud” is an infrastructure specifically designed for an organization that can be managed and located internally or externally.\textsuperscript{17} It is the most customizable option for an organization that offers the greatest security for stored data, if managed on a local network. The private cloud prohibits access by the public, which diminishes concerns of security breaches and data loss. Internal management of the software also protects defensibility in disputes that concern possession and control of information. With a private cloud, organizations can operate without interference from third-party liabilities. The increased control, however, eliminates some of the more beneficial aspects of cloud computing. By managing customized software on an internal network, an organization does not benefit from the decreased utilization of IT resources. As such, organizations have to perform a cost-benefit analysis, weighing control and security against ease and affordability.

The “Community Cloud” is an infrastructure developed for use by several organizations that share a common objective.\textsuperscript{18} This option is most used in areas where organizations work towards a similar goal. As in other cloud models, the community cloud provides access to an external network for users from varying endpoints. The benefit is a cost-effective alternative that promotes real-time productivity amongst adjacent organizations. The NYSE Technologies Capital Markets Community Platform (“Community Platform”) is a prime example of the community cloud. The NYSE Community Platform makes financial applications readily available to the capital markets community.\textsuperscript{19} Although each organization subscribed to the Community Platform has secured access to an individualized account, the data is stored in a shared infrastructure, managed by the provider. The community cloud is a tailored and narrowly focused model, aimed at a specific group; therefore, it does not face the same issues as a public cloud, which is open to the masses.

The “Hybrid Cloud” is an infrastructure that combines two or more of the other cloud models, held together by a standardized platform that enables the sharing of data.\textsuperscript{20} In the standard hybrid scenario, an external service provider manages a segment of the infrastructure, with the remainder managed by the internal network. For example, an organization can choose to store its archived information in a public cloud, while using a private cloud to securely store confidential information. Data that is less volatile can be harbored on a public platform, with proprietary data maintained on a private platform. By combining both private and public models, an organization can effectively minimize costs without jeopardizing security.

By understanding the characteristics of the various infrastructures, organizations can modify their use of cloud technology to enhance efficiency. Although most organizations

\textsuperscript{16} Id.
\textsuperscript{17} Id.
\textsuperscript{18} Id.
\textsuperscript{19} Community Platform (Cloud), NYSE Technologies (July 2013), http://nysetechnologies.nyx.com.
\textsuperscript{20} The NIST Definition of Cloud Computing, supra. at 1.
have already implemented some form of cloud computing, most operate without knowing
the risk that is inherent with sharing information over a foreign network. Once
organizations begin to acknowledge these risks, they can then begin to structure their
usage of the cloud in a manner that supports protection and security.

IV. ACCOUNTABILITY

In a recent report, the Cloud Security Alliance identified the top nine threats, challenging
cloud computing in 2013.\(^{21}\) The three greatest threats included data breaches, data loss,
and account hijacking, while malicious insiders and insufficient due diligence also made
the list.\(^{22}\) Based on this report, it appears as though both internal and external sources are
to blame for potential threats. While organizations can likely identify those accountable
for the internal breaches, information available for identifying the external breaches is
less certain. This dilemma becomes more troublesome when positioned in the context of
global commerce. Discrepancies in data protection laws amongst countries frame an
unstable environment in which organizations have to cooperate in order to ensure
the cross-border security of information. When this cooperation fails, what are the liabilities
and the remedies available to the affected parties?

a. THE UNITED STATES

The United States is home to some of the largest providers of cloud services, including
Google, Microsoft and IBM. Due to its dominance in the cloud market it is important to
understand the law that governs the operation of U.S. cloud providers and the affect is
has on the rights of non-U.S. customers subscribing to such services. It is equally
important to recognize the range of policy protections afforded in other areas of the
world, from heavy market contributors to emerging cloud markets, while focusing on
developing international initiatives aimed at standardizing data security.

The United States is a contract driven society. Most enforcement provisions are
embedded within service agreements, outlining the obligations and responsibilities of the
parties. A breach of that agreement often leads the injured party to seek damages by
initiating civil proceedings. Although there are federal and state laws that govern data
security, most focus on consumer protection, particularly in the areas of healthcare and
consumer finance. The private individual or organization is often left to its own devices
to follow applicable national regulations, while maneuvering through the plethora of
international laws, both country-specific and global. For this reason, organizations must
be careful in strategically developing contractual agreements to clearly identify the roles
of the involved parties. A lack of clarity in a contract, in conjunction with the lack of
clarity in the international laws that govern data security, will allow negligent parties to
avoid responsibility and accountability.

The greatest challenge for U.S. businesses in the global market for cloud computing is
convincing foreign users that the PATRIOT Act\(^{23}\) does not present a security risk to data
stored by U.S. cloud providers.\(^{24}\) Although the PATRIOT Act extends the government’s
access to stored data, it does not grant the government a blanket exception to obtain any

\(^{21}\) Cloud Security Alliance Warns Providers of “The Notorious Nine” Cloud Computing Top Threats in 2013,
The Cloud Alliance (Feb. 25, 2013), https://cloudsecurityalliance.org/media/news/ca-warns-providers-of-

\(^{22}\) Id.

\(^{23}\) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct

& Econ. 1, 16.
relevant information.\textsuperscript{25} According to the PATRIOT Act the government can gain access to stored information in two ways: FISA (Foreign Intelligence Surveillance Act) Orders and National Security Letters (NSL).\textsuperscript{26} The U.S. Federal Bureau of Investigation (FBI), in support of intelligence-gathering activities, uses FISA Orders to gather information concerning non-U.S. citizens and to protect against terrorism. Pursuant to Section 215 of the PATRIOT Act, a party that receives a FISA Order can be prohibited from informing its customers that their data was disclosed to the government.\textsuperscript{27} For obvious reasons, foreign users of U.S. cloud services fear that information could be released without their knowledge and without an opportunity to dispute such disclosure. On March 9, 2006, in response to these mounting concerns, the U.S. Congress enacted the USA PATRIOT Act Improvement and Reauthorization Act of 2005, which allowed recipients of a FISA Order to dispute the non-notification provisions of the Act.\textsuperscript{28} This provision would potentially alleviate some concerns because customers of cloud services would at minimum be notified when information was disclosed. FISA Orders, however, are rarely used, and as such, they do not pose a significant threat to customers of cloud services.\textsuperscript{29}

A NSL is another means available to the U.S. government to request stored information from cloud providers. It is a type of administrative subpoena, authorized by the head of an FBI field office, granting access to records that may be relevant to counterterrorism investigations.\textsuperscript{30} Authorization can be granted without the approval of a judge or jury and is likely granted in secrecy, prohibiting the recipient of the NSL from disclosing its contents to an affected party.\textsuperscript{31} In a recent decision, Judge Susan Illston, of the U.S. District Court for the Northern District of California, ruled that Google Inc. would have to comply with FBI issued NSL’s.\textsuperscript{32} The Judge, however, postponed her ruling until the 9\textsuperscript{th} U.S. Circuit Court of Appeals rendered its decision on whether NSL’s were constitutional.\textsuperscript{33} As such, the future use of NSL’s is yet to be determined.

Aside from the regulatory provisions that grant access to stored information, parties may seek a court-ordered subpoena or a search warrant through a civil litigation. This scenario should be the most troublesome to users of cloud services. In a dispute between two commercial parties, a provider of cloud services could be subpoenaed to produce information stored on behalf of a third-party non-litigant. This method, however, is not unique to the U.S. In France, both the Police Nationale and the Gendarmerie Nationale can execute search warrants, similar to those issued in the U.S.\textsuperscript{34} In Germany, Article 13 of the Basic Law also allows for judicial warrants.\textsuperscript{35} Comparatively, the risks that subpoenas pose in the U.S. market are paralleled in other markets within similar judicial proceedings.

\textsuperscript{26} Id.
\textsuperscript{27} Id.
\textsuperscript{29} Lakatos, supra.
\textsuperscript{30} 18 U.S.C. \textsection 2709.
\textsuperscript{31} Nickolas J. Bohl, Unsheathing a Sharp Sword: Why National Security Letters are Permissible under the Fourth Amendment, 86 B.U. L. Rev. 443 (2006).
\textsuperscript{33} Id.
\textsuperscript{34} Lakatos, supra.
\textsuperscript{35} Id.
The U.S., however, unlike the European Union (E.U.) and other market contributors, does not have a comprehensive data protection law, although it is moving towards promoting laws that protect privacy rights.\(^{36}\) On April 20, 2009, the Data Accountability and Trust Act (DATA) was introduced, and has since been referred to the Committee on Commerce, Science and Transportation.\(^{37}\) Presently, 42 states have breach-notice laws that require service providers to notify parties affected by security breaches.\(^{38}\) DATA would preempt state laws and provide a cohesive legal standard for the U.S., making providers responsible for reporting breaches to its customers.\(^{39}\) Additionally, large cloud providers and other interested parties have combined to form the Digital Due Process Initiative in 2010.\(^{40}\) The initiative promotes the standardization of communication and privacy rights, arguing that the current legal framework is outdated and noncompliant with evolving technologies.\(^{41}\) Although the future of these developments is uncertain, it is clear that U.S. service providers recognize the importance of offering a secure product to their customers.

b. THE EUROPEAN UNION

The E.U. is more advanced in its comprehensive regulatory scheme to manage data security. From Directive 95/46/EC, proposed in 1995, prohibiting the cross-border transfer of personal data, to the Data Retention Directive of 2006, which required service providers to retain certain data to be made available to law enforcement, the E.U. has attempted to protect data privacy through various regulations.\(^{42}\) On January 25, 2012, the E.U. revealed another proposed regulation to streamline the interpretation of these laws, increasing responsibility and accountability.\(^{43}\) Articles 5 through 7 incorporate several provisions of existing law, while adding conditions that would hold controllers of stored data liable for the mishandling of processed data.\(^{44}\) Specifically, Article 30 would hold both the controller and the processor of the data accountable for implementing adequate security safeguards.\(^{45}\)

The proposed regulation can have serious implications for providers of cloud services. Since current E.U. legislation requires providers that store data to conform to its security laws, all providers of cloud services with customers in the E.U. would then be held accountable, whether the data is stored within E.U. borders or abroad.\(^{46}\) The E.U. is a large market contributor, which acts as sufficient leverage to pressure cloud providers to conform to E.U. law. Companies wishing to take advantage of this market segment would have to implement security measures in compliance with E.U. regulations or risk liability.

c. INDIA

India is working on similar policy provisions in its legislature.\(^{47}\) Although India is considered an emerging market contributor, the growth is notably exponential, as supply


\(^{37}\) David Navetta, Potential Changes to the U.S. Breach Notification Risk Landscape, 7 Data Protection Law & Policy (Feb. 2010).

\(^{38}\) Id.

\(^{39}\) Id.

\(^{40}\) Berry, supra. at 17.

\(^{41}\) Id.

\(^{42}\) Navetta, supra. at 13-17.

\(^{43}\) Francoise Gilbert, European Data Protection 2.0: New Compliance Requirements in Sight, IT Law Group (Feb. 08, 2012).

\(^{44}\) Id. at 7-8.

\(^{45}\) Id. at 15.

\(^{46}\) Berry, supra. at 11.

\(^{47}\) Id. at 13.
and demand for cloud services is on a rapid increase. Recent forecasts project the market for cloud services to reach $1.08 billion by 2015, up from $110 million in 2010.\textsuperscript{48} Considering these figures and the extent of India’s influence in the technology market, it is evident that India will play a critical role in the expansion of cloud services.

Like the E.U., India has enacted various laws to create a comprehensive regulatory scheme to standardize the protections which relate to electronic data. The Information Technology Act of 2000 (IT Act), as amended in 2008, regulates the management of communications transferred through the Internet.\textsuperscript{49} The greatest concern for cloud service providers operating in India is Section 43A of the IT Act. It states that when any organization, “possessing, dealing, or handling” stored information, “which it owns, controls, or operates, is negligent in implementing and maintaining reasonable security practices and procedures,” it will be held liable for its misconduct.\textsuperscript{50} An understanding of the “reasonable security practices” necessary to avoid liability remains uncertain.\textsuperscript{51} The consequence of this uncertainty may heighten the enforcement of security measures as providers of cloud services attempt to proactively prevent violations of the IT Act.

In 2013, to further address data privacy concerns, the Indian government released the National Cyber Security Policy (NCSP).\textsuperscript{52} The NCSP outlined a list of objectives aimed to ensure compliance with global security standards.\textsuperscript{53} As it relates to cloud services, the NCSP sought to enable the protection of information in the cyber-sphere while investigating and prosecuting potential violations.\textsuperscript{54} The NCSP further sought to mandate the implementation of a security audit that would periodically monitor the safeguards utilized to secure sensitive cyber infrastructures.\textsuperscript{55}

A simultaneous application of the NCSP and the IT Act would suggest that providers of cloud services, operating in India, could be held liable for failing to provide reasonable security measures as prescribed by global standards. Therefore, a U.S. company, such as IBM, that is storing information for an Indian entity, may be held liable for maintaining inadequate defense protocols to combat potential threats, even if those protocols would be in compliance with U.S. law. Similarly, if information transferring through a network serviced in the E.U. is mishandled, the E.U. provider could be held accountable even if its procedures were in accord with E.U. regulations. These implications can complicate growth of cloud services in India, as providers are forced to cautiously maneuver through this legal framework. Based on market projections, however, this seems unlikely as growth will continue.

d. CHINA

Similar to India, China is considered an emerging contender in the market for cloud services, which remains underdeveloped.\textsuperscript{56} China differs from India, however, in that it does not have a comprehensive data security law.\textsuperscript{57} In recent years, however, Chinese regulators have attempted to draw technological investment into the country by

\textsuperscript{50} Id. at 43A.
\textsuperscript{51} Berry, supra. at 30.
\textsuperscript{52} National Cyber Security Policy, No. 2(35)/2011 (2013) (India).
\textsuperscript{53} Id. at 3.
\textsuperscript{54} Id. at 4.
\textsuperscript{55} Id. at 8.
\textsuperscript{57} USDOC, supra.
modifying the legislature to extend protections to electronic data. “Several Regulations on Standardizing Market Order for Internet Information Services” was passed in 2011, followed by the Decision of the Standing Committee of the National People’s Congress to Strengthen the Protection of Internet Data in 2012, and the Information Security Technology — Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems in 2013.

The 2011 Regulations, enacted by the Ministry of the State Council, narrowly applied to Internet Service Providers and Internet Information Services. Providers that came within the provisions of the Regulations were required to safely store collected data and take “prompt remedial measures” to reduce risk of loss. Any provider in violation of this requirement could be subject to a fine, ranging from roughly $1,500 to $4,800. The penalty for non-compliance under the Regulations seems to be a non-threatening consequence that may fail to deter violations.

Decisions rendered by the Standing Committee have a greater legal effect than those promulgated by the Ministry. As such, the 2012 Decision weighs more heavily in the legal context than the 2011 Regulations. Although the 2012 Decision covers many of the same topics as the Regulations, it expands to apply to any Internet content provider who collects or uses data. The Decision is phrased in general terms, but it does specify the obligation to provide adequate security measures, though it is unclear whether a violation would result in absolute liability or whether negligent conduct would be required to claim damages. If a breach occurred, the violator would be required to contact the “relevant competent agency” that would investigate and take enforcement action. Language in the Decision suggests that civil damages, however, would have to be sought in a claim under Tort Liability Law.

The most recent Guidelines issued in 2013, although having the least legal significance, may be the strongest indication of China’s perspective on data security. These Guidelines apply to the broadest ranges of businesses, outlining a number of basic principles that should be followed in the data protection process. Most notably is the “clear responsibility principle,” which requires organizations to clearly define responsibilities and to record processing strategies. This principle would act as an evidentiary tool to guide in the investigation of violations.

Read together, the documents do not clearly address issues of accountability. Although each requires some level of enhanced security, it is unclear at what point a cloud service provider would be held liable. The documents do not define or specify the technical standards necessary to be in compliance with the security provisions. Considering that

---

59 Id.
60 Id.
61 Graham Greenleaf, China’s NPC Standing Committee Privacy Decision: A Small Step, Not a Great Leap Forward, University of New South Wales Faculty of Law Research Series 2013, (April 2013).
62 Id. at 2.
63 Id. at 3.
64 Id. at 4.
65 Id. Decision states that violators shall be subject to civil liability in accordance with the law and any person whose rights were affected can seek restitution through litigation.
67 Id. at 4.
68 Id.
most providers of cloud services implement some of the safest data security systems, it appears that it would be difficult to come under the enforcement provisions of the law. Nevertheless, the tailoring of its laws to provide increased security is a clear indication that China expects to increase its presence in the market for cloud services. As such, additional changes to this area of the law should be expected in the future.

V. INTERNATIONAL GUIDELINES

Due to the apparent jurisdictional differences, efforts have been made to formulate international guidelines, which would aid the market for cloud services in properly developing management and enforcement policies. As with most international law, the difficult factor in its formation is the adoption by all relevant parties. Without global cooperation, however, it would be futile to attempt to enforce these efforts.

The Guidelines formulated by the Organization for Economic Cooperation and Development (OECD), adopted in 1980, became the first multilateral agreement to establish data rights with principles to protect these rights.69 In particular, Article 16 required that Member countries take “reasonable and appropriate steps” to ensure that the flow of data across borders was “uninterrupted and secure.”70 The Guidelines, however, did not include provisions that addressed issues of accountability. As such, Member countries were still left to seek country-specific resources to regulate conflicts.

Perhaps, in light of the lack of enforceability measures found in other international agreements, the Asia-Pacific Economic Cooperation (APEC) developed the 2004 APEC Privacy Framework, targeting responsibility and accountability.71 The purpose of the Framework was to make those who handled stored information responsible for any loss or damage.72 By focusing liability onto service providers, Member countries could promote the implementation of enhanced security measures. With this international definition, regulating standard practice policies, the Framework would act to level the playing field in which providers could operate in various jurisdictions without fear of liability.

In a more recent effort to promulgate international data security principles, the 50 countries that participated in the International Conference of Data Protection and Privacy Commissioners in 2009, not including the U.S., developed the Madrid Resolution. More akin to the E.U. Directive discussed previously, the Madrid Resolution outlined principles necessary to protect the trans-border flow of data. Importantly, however, the Resolution was a nonbinding agreement, thus, its adoption had little effect on enforceability.

VI. CONCLUSION

The growth and significance of cloud computing in the current global market is undisputable, and based on recent studies, it is only expected to grow. As a cost-saving alternative to complex internal IT infrastructures, organizations look to the cloud to alleviate data storage concerns. Many, however, are apprehensive of the implementation of a cloud driven network. Considering the cost and frequency of service interruptions and data breaches, these hesitations may have merit.

As many previous evolutions in technology have proven, the development of a new software or device brings with it countless uncertainties. The cloud, however, is not

---

70 Id.
72 Id.
necessarily a new development. For years prior to the growth of the cloud, people sent e-mails using their smartphones without questioning where that information and any attached documents were being stored. It is no surprise that in order to be able to grant continued access to that document, the telephone service provider had to store the information in a cloud. Similarly, when an organization purchased software that operated over the Internet, the information collected during the use of that software was stored in a cloud. Now that cloud services are being offered in bulk and in substitute of internal storage options, organizations are becoming anxious about trusting a third-party provider. The market, however, must learn to evolve and adapt to new technologies just as it did with the introduction of the Internet and the wireless smartphone.

To guide in this evolution, the trend in recent years has been to promote data security. Most countries have enacted some form of legislature to govern the management of information that is transferred through the Internet or that is stored in a remote server. In recognition of the importance of secure data maintenance, international organizations have also enacted guidelines and principles that set a standard for global market participants. Although commendable, these efforts have not yet resulted in a comprehensive legal standard that mandates certain acts, while holding violators of those acts accountable for their breaches.

The question then becomes, who is responsible?

Based on the current legal framework, the answer remains unclear. The lack of clarity, however, highlights the significance that contract negotiations have on the legal remediation available to users of cloud services. An organization considering the implementation of a cloud service should carefully and strategically construct the service agreement to include clauses that would hold the provider liable for any negligent or intentional security breach. The contract should specifically set forth the responsibilities of the provider that are required to effectively perform the provisions of the contract. Any failures thereof should result in defined ramifications. The parties should also clearly define what constitutes a breach, which would eliminate future disputes in determining whether the party suffered damages.

Presently, most service providers draft contracts to limit liability. For example, in the Customer Agreement for Amazon Web Service (AWS), Section 10 states:

The service offerings are provided “as is”… we and our affiliates and licensors make no representations or warranties of any kind…including any warranty that the service offerings or third party content will be uninterrupted, error free or free of harmful components, or that any content, including your content or the third party content, will be secure or not otherwise lost or damaged.73

Similarly, in the Terms of Service for Google Cloud Storage, Section 13 states:

Except as expressly provided for herein, to the maximum extent permitted by applicable law, Google does not make any other warranty of any kind…Google is not responsible or liable for the deletion of or failure to

store any content and other communications maintained or transmitted through use of the Service…Google does not warrant that the operation of the software or the Service will be error-free or uninterrupted.74

This contract language clearly shows how the intent of service providers differs from the intent of regulators. The former limit liability while the latter act to promote confidence and security.

The questions that remain unanswered, however, should not be considered an obstacle to prevent organizations from utilizing a cloud service. Rather, they should, act as a warning to caution users of the potential risks that threaten stored information. By taking cautionary measures to properly implement cloud services, organizations can eliminate some of these risks, while still being able to reap the benefits. To do so, business leaders must first become familiar with cloud technology and the market for cloud services. Only then will organizations be able to properly and securely use the cloud. In the words of Thomas Jefferson, “To penetrate and dissipate these clouds of darkness, the general mind must be strengthened by education.”

***

Vincent M. Catanzaro is Senior Counsel, Global Discovery Manager for E. I. du Pont de Nemours and Company. In this role, Vince is responsible for counseling the Company concerning how best to comply with evolving legal standards relating to discovery, guiding and supporting the legal teams in the development of e-discovery response strategies and the use of litigation technology, coordinating, managing and monitoring the work of the Company’s discovery vendors and overseeing DuPont Legal’s Discovery Excellence Center. Before assuming this role, Vince worked with various DuPont litigation groups specializing in discovery management and consulting on the development of DuPont’s Discovery Policies and Guidelines.

Prior to joining DuPont, Vince practiced in suburban Philadelphia where he concentrated on Construction Litigation on the state and federal level. He represented a diverse client base from industry suppliers to individual contractors in contract disputes, design interpretation, zoning matters and sales agreements.

A dual citizen of both the United States and Italy, Vince has been active in community, cultural and professional organizations as he is currently a member of the National Italian American Bar Association and National Order of the Sons of Italy. He is a current member of the Sedona Conference Working Group on Electronic Document Retention and Production, a former faculty member of the Georgetown Law School Advanced e-Discovery Institute and Academy, a member of the Richard Herrmann Technology Inn of Court, a Certified Six Sigma Green Belt and an Adjunct Professor of eDiscovery at Widener University Legal Education Institute. Vince has co-authored an article for the ACC Docket Magazine with Jonathan Redgrave, entitled, “Managing the Emerging Business and Legal Realities of Social Media in Corporate America” and an article for the International In-house Counsel Journal entitled “Shhh- the Internet is listening: Has technology eroded Attorney-Client Privilege and what can You do about it?”.

Vince received his undergraduate degree from Temple University and his Juris Doctor from Widener University School of Law where he served on the Student Bar Association and the Legal Skills Committee. He is admitted to practice in the Commonwealth of Pennsylvania, the State of New Jersey, the Eastern District of Pennsylvania and the State of Delaware for the limited practice of law as in-house counsel.

Karine Tatoyan is a member of the Pennsylvania Bar. She graduated with honors from the Villanova School of Business and the Widener University School of Law. Since her graduation in 2012, Karine continued work in the business sector, focusing on regulatory enforcement of legislative provisions in the real estate market. While at Widener Law, Karine received The Lucinda Peipher Memorial Award, an academic achievement award...
for outstanding performance in International & Business Law. Karine also competed in the 2012 Philip C. Jessup International Law Moot Court Competition, the world's largest moot court competition with participants from over 500 law schools in more than 80 countries. Although a native of Ukraine, Karine grew up in Philadelphia from age five. She is fluent in Russian and is proficient in Spanish. Combining this interest of culture, business and the law, Karine completed a yearlong Public Interest Externship with DuPont Legal, an international organization where she worked in the Discovery Excellence Center and gained exposure to all areas of the law. Presently, Karine hopes to continue her career in international business law, utilizing studied world legal knowledge and the innovation of her generation.

**DuPont (NYSE: DD)** has been bringing world-class science and engineering to the global marketplace in the form of innovative products, materials, and services since 1802. The company believes that by collaborating with customers, governments, NGOs, and thought leaders we can help find solutions to such global challenges as providing enough healthy food for people everywhere, decreasing dependence on fossil fuels, and protecting life and the environment.