Journal of Technology Law & Policy

Volume 16 | Issue 2 Article 2

December 2011

Cloud Computing Prividers and Data Security Law: Building Trust with United States Companies

Jared A. Harshbarger

CLOUD COMPUTING PROVIDERS AND DATA SECURITY LAW: BUILDING TRUST WITH UNITED STATES COMPANIES

Jared A. Harshbarger[*]

---

* Jared A. Harshbarger, a former in-house attorney and corporate legal counsel to multiple Fortune 500 international companies, is currently providing legal and business consulting services in the fields of intellectual property and emerging technologies. He has a Master's of Business Administration (MBA) from University of Iowa in Iowa City, Iowa, USA; a Master's of Law (LLM) in Innovation, Technology and the Law from the University of Edinburgh School of Law in Edinburgh, Scotland, United Kingdom, through the SCRIPT Research Centre for Studies in Intellectual Property and Technology Law, sponsored by the Arts and Humanities Research Council of the British Parliament. In addition, the author earned his Juris Doctor degree (JD) from Thomas Jefferson School of Law in San Diego, California, USA; and his Bachelor's degree in Liberal Studies with a minor in Physics from Iowa State University in Ames, Iowa, USA. A very special thank you to the author's beautiful wife, Ann, whose truly special contributions to the world—and unparalleled love for her fellow man—can never be overstated.

INTRODUCTION

"Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry . . ."[1]

Cloud computing is being hailed as the future of information technology (IT) architecture. It is projected that by the year 2018, service-based solutions will be a major medium for delivery of information and other IT functions at both the consumer and corporate ranks.[2] Cloud computing transfers the application software and server-based databases to the centralized large data centers, where the security measures taken by cloud providers to safeguard the data entered into the cloud may not be fully trustworthy.[3] With the explosion of data being entered and managed by electronic means and the increasing prevalence of identity theft cases, data security for consumers and businesses sharing their data in the cloud is paramount.

The young archetype of cloud computing brings about many new legal challenges, given the breadth of data breaches and fluid creation of new laws and regulations in the United States and abroad. While privacy and data security are closely linked, they are slightly different in terms of legal obligations and approach. As such, privacy will not be the focus here. This Article studies the issues that cloud computing providers face in ensuring the integrity and security of data storage in the cloud and how those cloud providers can build trust among potential and existing U.S. company customers.

Due to its brief history, there has not been extensive research published or comprehensive review on cloud computing. The issues created by cloud computing are new and still open for debate among scholars and, more importantly, for the data holders, and the judicial and legislative bodies. Thus, the domain of research available to write this is rather thin. While challenging to find established research on cloud computing, this Article attempts to prompt further discussion on the new legal issues raised by this topic.

Various state and federal laws mandate a wide variety of security

---

1. Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing*, (Univ. of Cal. at Berkley, Technical Report No. UCB/EECS-2009-28 2009), http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

2. Mladen A. Vouk, *Cloud Computing-Issues, Research and Implementations*, 16 J. COMPUTING & INFO. TECH. 235, 236 (2008), http://cit.srce.hr/index.php/CIT/article/viewFile/1674/1378.

3. *See* Qian Wang et al., *Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing*, *in* 5789 LNCS, EUROPEAN CONFERENCE ON RES. IN COMPUTER SECURITY 355 (2009).

requirements for the holders of certain data to ensure privacy and prevent identity theft, among other worries. For U.S. companies to ensure the trust of their customers and avoid litigation, compliance with these laws and regulations is a must. If the subject data is shared with a third party cloud computing provider, the company must ensure that the provider will maintain the company's data security obligations.[4]

However, this outsourcing of data storage and processing does not relieve the company of its data security obligations. Rather, the company remains liable for potential breaches of the data being exposed to outside persons. Thus, the U.S. companies that employ cloud computing as a method for doing business must perform the due diligence on, and obtain the contractual obligations from, the cloud providers they utilize. U.S. companies are pressed to gain written assurances that they can trust the cloud provider and perhaps relieve themselves of certain liabilities. It is this trust that cloud providers must create and implement for the cloud computing model to be successful. As I will assert herein, there are reasons for needing this trust and solutions for gaining it.

I. WHAT IS CLOUD COMPUTING?

Cloud computing is an IT architectural trend in the computer industry. "Rich Zippel of Sun Microsystems labeled cloud computing as 'the hottest, and certainly the most abused, buzzword in computing today.'"[5] There is much debate about the precise definition, but essentially, cloud computing means remote computing with software and databases accessed through the Internet.[6] These software applications and databases are predominantly funded by the amount that is used in a certain timeframe.[7] Cloud computing pioneers have existed for years, but the phrase became popular in 2007 when IBM and Google collaborated for a new project.[8] This was followed by IBM's announcement of its "Blue Cloud" as well as Google's dramatic increase in applications provided on their "cloud."[9]

---

4. *See* MD. CODE, COM. Law. § 14-3503(b) (2011) (effective Jan. 1, 2008).

5. Miranda Mowbray, *The Fog over the Grimpen Mire: Cloud Computing and the Law*, 6 SCRIPTED 129, 133 (2009).

6. *Id.*

7. *Id.*

8. *See generally Google and IBM Announce University Initiative to Address Internet-Scale Computing Challenges*, IBM (Oct. 8, 2007), http://www-03.ibm.com/press/us/en/press release/22414.wss (establishing an initiative to tackle "scale computing challenges" which would later be referred to as cloud computing).

9. *Seeding the Clouds: Powerful New Provisioning, Monitoring, and Management Drives IBM Blue Cloud*, IBM http://www-01.ibm.com/software/tivoli/beat/03112008.html (last

Users of the cloud go from the prior and existing system of performing computing practices on their own hardware and using copies of software that they own, to users performing computing practices on an outside vendor's machines somewhere in the cloud and utilizing software that the user rents.[10] Cloud computing is based on what can be called "cyber infrastructure, and builds upon decades of research in virtualization, distributed computing, 'grid computing,' utility computing, and, more recently, networking, web and software services."[11] Cloud computing is a service-oriented architecture; it reduces IT overhead, allows increased flexibility, and reduces the cost of a user's computing practices.[12]

The main concept of cloud computing services is that these services are carried out on behalf of users with hardware that the customers do not own or operate.[13] The user inputs data to the cloud, the data are processed by the cloud service provider according to the instructions of the user, and the output is delivered back to the user.[14] The services in the cloud computing industry can be referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS).[15] Furthermore, cloud computing allows these new services to be used in the cloud with other services. For example, a "print on demand" service could be provided by combining a printing service with a storage service.[16]

Regardless of the definition you choose, the main difference with traditional computing and cloud computing is that the user transitions from operating on their own mainframe to operating on an Internet-based architecture in the "cloud." One good example of this is Google's suite of applications including: the popular Gmail, Google documents (where word-processing and spreadsheet documents can be created and saved), Picassa (for photo storage and manipulation), and even Google Health (where the user can manage their medical records). To illustrate further, some additional common and growing cloud-based platforms

---

visited Sept. 24, 2011).

10. Mowbray, *supra* note 5, at 133.

11. Vouk, *supra* note 2, at 235.

12. *Id.*

13. Miranda Mowbray & Siani Pearson, *A Client-Based Privacy Manager for Cloud Computing*, 4 PROC. INT'L ICST CONF. ON COMM. SYS. SOFTWARE & MIDDLEWARE 5, § 1 (2009).

14. *Id.*

15. Rajkumar Buyya et al., *Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities*, 7 PROC. HIGH PERFORMANCE COMPUTING & SIMULATION CONF. 1, 1 (2009) (keynote paper).

16. Siani Pearson, *Taking Account of Privacy when Designing Cloud Computing Services* § 3.1 (Hewlett Packard Labs., HPL-2009-54, 2009), http://www.hpl.hp.com/techreports/2009/HPL-2009-54.pdf.

include social networking (*i.e.*, Facebook or MySpace), web hosting, content delivery, and real-time data processing.[17] Chances are that cloud computing has already entered your life and daily activities, whether at your job or in your personal life.

II. ADVANTAGES OF CLOUD COMPUTING

Currently, almost every business uses and relies upon some form of IT and IT services. In the prudent corporate environment today, these services require an economy-of-scale, comparing the cost-of-ownership against utilizing a cloud computing provider.[18] A successful corporate IT department needs to improve end-user productivity while reducing IT overhead.[19] To illustrate, unless IT is the primary business of a corporation, less than 20% of its efforts not directly connected to its primary business should have to do with IT overhead—even though 80% of its business might be conducted using electronic means.[20] This 20/80 rule is very common and should apply to most every non-technology-selling corporation.

The cost of IT overhead can be substantial. License fees, maintenance fees and professional service fees come at a premium for those wishing to house their IT services solely in-house. In addition, physical, on-site data centers come with high operating costs. From enterprise software licensing to purchasing and implementing the hardware needed to run the software, U.S. companies are faced with a tough choice: own their infrastructure or outsource to a cloud computing provider. There are several benefits to choosing a cloud computing provider which are discussed below.

Cost savings are at the forefront of nearly every company's budgeting process. With cloud computing, internal software developers and the corporations they work for would no longer be required to make large capital expenditures in the hardware and software infrastructures to deploy their IT services to the company; the cloud provider already has those in place. There is no need for physical security as there is not a requirement for a company data center. Also, the employee man-hour labor expense to train, implement, and maintain such an infrastructure is eliminated because the cloud provider has its own dedicated staff to provide support.[21]

---

17. Buyya et al., *supra* note 15, at 1.

18. Vouk, *supra* note 2, at 236.

19. *Id.*

20. *Id.*

21. *See* Armbrust et al., *supra* note 1, at 12 (discussing the elasticity of using cloud computing compared to the cost of maintaining an on-site server, which must have capacity that

Cloud computing offers significant benefits to companies by liberating them from the basic job of setting up hardware and software infrastructures, and in turn, enables their employees to focus more on their company's business.[22] Cloud computing is particularly appealing to companies facing financial recessions because using cloud services allows them to substitute capital expenditure on the hardware and software needed to meet their worst-case computing requirements with operating expenditure that only relates to the amount of IT-related services that they actually use.[23] To make matters easier for customers, cloud providers can allow the user to just increase computing capacity on-demand, eliminating any burdensome hardware and software additions. With license negotiations, hardware delivery and installation taking several months on average, the instant and real-time capacity increase of cloud computing saves the company valuable time and cost.[24]

In addition, scalability becomes a positive factor in choosing to do business through a cloud computing provider. Increased network bandwidth and reliable network connections make it possible for companies to subscribe to IT services that reside solely on remote data centers.[25] The cloud provider is responsible for the computing resources necessary to support all of its customers, likely ensuring that all of a company's necessary bandwidth is available. Furthermore, common needs among a cloud provider's customers can be built into their software one time, allowing for instantaneous access to everyone. This scalability alleviates the concern for a company to internally compensate for all of the possible computing power it *may* need.[26]

Indeed, cloud computing has grown to posture itself as a new model for providing reliable access to scalable IT services.[27] The objective of cloud providers is to give users the ability to program resources within a very large-scale resource cloud so that they can take advantage of the potential performance, cost, and reliability benefits that access to scale makes possible.[28]

The cloud model is even more attractive to small businesses that often lack the required capital to implement an IT department or even

---

is rarely used).

22. Buyya et al., *supra* note 15, at 1.

23. Mowbray & Pearson, *supra* note 13.

24. Armbrust et al., *supra* note 1, at 4.

25. Wang et al., *supra* note 3, at 355-56.

26. Armbrust et al., *supra* note 1, at 12.

27. *See* Daniel Nurmi et al., *Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems*, § 1 (UCSB Computer Sci. Tech. Rep. No. 2008-10, 2008), http://open.eucalyptus.com/documents/nurmi_et_al-eucalyptus_tech_report-august_2008.pdf.

28. *Id.*

implement the necessary IT infrastructure to do business. Salesforce.com is an example of one cloud computing provider that allows small and medium-size companies the IT functionality they could not otherwise afford to utilize.[29] Another resource that is predominantly free for small businesses is the suite of applications created and run on Google's cloud.

While there are many benefits to cloud computing as described above, there is one glaring benefit that companies cannot ignore: the outsourcing of data storage and other data-infused business. This outsourcing allows for a particular company to potentially transfer liability for data breaches to the third party cloud provider. It follows that, while the company that receives or creates the data is still responsible for its security, they may contractually bind the third party cloud provider with the company's security obligations and have a source of relief in the event of a breach. This pass-through liability transfer is becoming more and more common and is the very issue of the trust theme upon which this Article is based.

The benefits of cloud computing can only be realized by companies if they feel confident that the cloud provider will not expose them to liability, regardless of whether they are shielded legally from it; a breach of data security can be very expensive to remedy and carries with it a costly negative connotation in the mind of the consumer. Thus, even though the advantages are great, cloud computing has one important disadvantage regarding data security that must be addressed by cloud providers to both grow their own business as well as to ensure the viability of the cloud computing model of operation.

III. DISADVANTAGES AND DATA SECURITY ISSUES IN CLOUD COMPUTING

Data security has become a fast-growing concern for U.S. companies and consumers alike. The security of one's data is a complex issue that reaches virtually all people and companies. Private, confidential, proprietary, secret, undesirable, and damaging information is memorialized in electronic form all across the Internet and the world. When it comes to cloud computing, data security is probably the most sensitive issue with those deciding whether a party will trust the cloud provider with their data. This is because the data owners possess a personal and/or business interest in keeping their data protected from outside or unintended access. Furthermore, when such data from consumers is entrusted with a company in the United States, the

29. Steve Mansfield-Devine, *Danger in the Clouds*, NETWORK SECURITY, Dec. 2008, at 9.

company must comply with those laws and regulations to prevent access.

Trusting a cloud provider with the data that are subject to such laws and regulations requires a great amount of trust and assurance. This is not without just cause. There are privacy concerns such as identity theft, trade secret divulgence and other malicious acts that data could be subject to. Cloud providers may or may not have the proper security measures in place to not only comply with the laws and regulations, but also to provide the data owner that warm and cozy feeling that their data is secure and free from outside exposure. Furthermore, this feeling is greatly desired because of several factors that weigh heavily on the minds of the data owners and that relate to data security.

First, cloud computing providers offer a very convenient target for hackers.[30] Rather than a traditional company housing its own data alone which is mostly accessible only internally, a cloud provider houses many times more data all in one site which is available from anywhere. Companies realize this one-stop-shopping for hackers when trusting their data to a cloud computing provider. "'Traditional systems are masked behind firewalls [and other gateway boundaries], so attackers must do intensive intelligence gathering to know that they exist,' explains Greg Day, security analyst at McAfee."[31] "'Last year, Monster was hacked and millions of contact details stolen which unleashed a phishing attack,' says Day. 'When it comes to business services in the cloud, the cyber criminal only needs to hack one site to get access to multiple companies.'"[32]

Second, if access software is needed on the user-end, not promptly installing upgrades or updates made available by the cloud provider could result in increased vulnerability and decreased data security. In addition, the user is at the mercy of the cloud provider to effectively communicate and notify the user of the new upgrade or update.

But, perhaps the most important data that could be entrusted with a cloud computing provider are that of personally identifiable information (PII). The different data security laws and regulations discussed below define PII in their own way. However, most have the common theme that PII is someone's name, coupled with vital information such as their social security number, account numbers or even personal health information. Identity theft can be one of the most serious crimes committed depending on how the hacked data is used. Potentially, thousands of dollars on new credit cards may be quickly accumulated and other fraud-related activities can transpose every day. High-profile

30. *Id.*
31. *Id.*
32. *Id.*

data breach lawsuits receive serious attention.[33] Primarily, this is because these crimes can severely damage the data owner's credit, financial stability and maybe even their entire well-being. The United States has seen several data breach lawsuits of note. For instance, in 2007, TJX was hacked to the tune of over 45 million customer credit card numbers.[34] In 2008, MasterCard suffered a similar breach in data security costing them over $41 million.[35] In addition, there have been several prominent cases relating to lost or stolen laptop computers containing sensitive data.[36] These criminal acts cost companies vast amounts of dollars and invaluable reputation and cost banks and credit card companies millions of dollars in refunds for fraudulent charges.[37] As a result of the rise of identity theft, consumers and companies focus more and more on to whom and how they divulge PII.

Cloud computing providers may be vulnerable to a data breach at any time. The security measures the cloud provider has in place are not required to adhere to any standard, nor are they subject to any other form of oversight. When a company uses a cloud computing provider, they do so at their own risk. Data security is, and will always be, one of the largest risks facing U.S. companies who collect data from consumers. Thus, employing an outsourced cloud provider that will be receiving such data certainly requires a qualified level of trust and assurance.

One additional note worth mentioning is the U.S. Patriot Act and its effect on cloud computing providers.[38] The U.S. Government may potentially gather data in the cloud.[39] As such, the trust and use of cloud computing services presents a risk for any company. The fear of the U.S. Government snooping has already had a negative effect on Google.[40] Similar measures are in place in the United Kingdom via the Regulation of Investigatory Powers Act and in other jurisdictions.[41]

---

33. Pearson, *supra* note 16, § 2.3.

34. Bill Brenner, *Banks Prepare Lawsuit over TJX Data Breach*, SEARCHFINANCIAL SECURITY.COM (Jan. 17, 2008), http://searchfinancialsecurity.techtarget.com/news/1294453/Banks-prepare-lawsuit-over-TJX-data-breach.

35. *MasterCard Settles with Heartland*, YAHOO! FINANCE (May, 21, 2010, 10:47 AM), http://www.zacks.com/stock/news/34541/MasterCard+Settles+with+Heartland.

36. Julie Machal-Fulks & Robert J. Scott, *Laptop Data Breaches: Mitigating Risks Through Encryption and Liability Insurance*, SCOTT & SCOTT § II, http://www.scottandscottllp.com/main/uploadedFiles/resources/Articles/Article-Laptop_Data_Breaches.pdf (last visited Sept. 28, 2011).

37. Brenner, *supra* note 34.

38. *See* USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 278 (codified as amended at 42 U.S.C. § 2516 (2006)).

39. *Id.*

40. Paul T. Jaeger et al., *Cloud Computing and Information Policy: Computing in a Policy Cloud?*, 5 J. INFO. TECH. & POL. 269, 276 (2008).

41. Regulation of Investigatory Powers Act, 2000, c. 23, § 3-5.

U.S. companies that want to prevent the unauthorized disclosure of data to another "country's government would be wise to avoid using cloud computing services that process or store data in that country."[42] As such, a cloud computing provider could try to limit or eliminate utilizing servers in such countries (although it certainly seems impractical to eliminate operations in the United States or United Kingdom).

PII that is given to a U.S. company (from its customers or employees) must be exposed to the appropriate level of protection throughout the data's chain of custody. The company that a data owner divulges its PII to has the liability under the various state and federal laws to maintain the security of that data. Even though a company may use a cloud provider, the liability still remains with that company. However, if the data is shared with a cloud provider, the company may obtain liability relief from that provider. As such, cloud computing providers must take their acceptance of PII and other information very seriously and adhere to the same laws and regulations regarding such data as the company itself. Otherwise, the company most likely would not choose to use that cloud provider's service, fearing the potential for that cloud provider to violate a law or regulation. Through representing and/or warranting compliance with applicable laws and regulations *vis-à-vis* contract, as well as other actions (as will be discussed in greater detail later in this Article), cloud providers can start the important task of building trust among U.S. company customers to gain their business and ultimately achieve success as service providers and as an industry.

IV. DATA SECURITY LAWS AND REGULATIONS FOR U.S. COMPANIES

The most straight-forward manner in which a computing provider can begin to build the trust of a U.S. company is to represent and/or warrant compliance in a service contract with the laws and regulations incumbent on that company. This is because it gives the company a legal remedy in case of a data breach, civil fine or injunction occurring as a result of the data being in the control of the cloud provider. If it is determined that data entrusted to the cloud provider was subject to applicable laws or regulations and the company is sued, fined or subject to an injunction as a result, then that company can recover through breach of contract with the cloud provider.

But, what laws and regulations must cloud computing providers represent and/or warrant that they comply with? How do they comply?

42. Mowbray, *supra* note 5, at 135.

While there are many countries and districts within those countries that have their own unique laws and regulations regarding data security, this Article will only focus on the prominent ones that U.S. companies potentially must abide by. As you will see, many of these laws mandate similar security requirements and are mostly limited to the same or very similar sort of PII collected. Thus, compliance is not as difficult as developing a separate policy for each one. Rather, data security compliance most likely hinges on a comprehensive policy that encompasses the general requirements, and depending on the situation and data collected, the specific requirements that are present throughout these laws and regulations. This practice is definitely less daunting then complete global compliance and should be very manageable for cloud computing providers to implement in order to build trust with U.S. companies that they want to do business with.

A. *U.S. Federal Laws*

The first level of legal regulation regarding data security in the United States comes from two main laws and is supplemented by one other law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs the security of consumers' health-related data.[43] The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLB), protects consumers' personal financial information given to financial institutions.[44] In addition to these two Acts, the Flag Rules supplement creditors and financial institutions' responsibilities to prevent and manage identity theft.[45]

1. HIPAA

HIPAA was enacted in the United States to simplify the administration of health insurance claims and lower costs, give patients more control and access to their medical information, and protect individually identifiable medical information from real or potential threats of disclosure or loss.[46] Title 2 of the HIPAA regulations addresses the control of medical records.[47] Under this section, the Department of Health and Human Services sets the Standards for Privacy of Individually Identifiable Health Information.[48] It specifies

43. 42 U.S.C. § 1320d-6 (2006).

44. 15 U.S.C. § 6802 (2006).

45. 16 C.F.R. § 681.1 (2011).

46. David C. Kibbe, *A Problem-Oriented Approach to the HIPAA Security Standards*, FAM. PRAC. MGMT., July-Aug. 2001, at 37, 38, *available at* http://www.aafp.org/fpm/2001/0700/p37.pdf.

47. *See* 42 U.S.C. §§ 1320d-1 (2006).

48. Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the*

that 18 data points, known as protected health identifiers (PHI), that could possibly identify a patient, must be appropriately protected from disclosure.[49] This requires PHI holders to use "reasonable and appropriate" means to ensure that: (1) administrative safeguards are in place to manage the selection and execution of security measures; (2) physical safeguards are in place to protect electronic systems and related buildings and equipment from environmental hazards and unauthorized intrusion; (3) technical safeguards are in place, including automated processes to protect data and control access to it; and (4) risk assessments conducted and security policies and procedures are documented.[50] To the first and fourth points, this means documenting your security practices and having policies in place that address such measures as data back-up, disaster recovery and who has access to the PHI.[51] Physical safeguards include making sure computer monitors are not in easy view of others, automatic computer logout for inactivity, limiting personnel who have access to PHI, ensuring complete destruction of PHI when it is no longer needed and having doors and files locked where PHI is kept.[52] Technical safeguards are perhaps the most relevant to cloud computing providers and include such measures as passwords and keys, unique identification, digital signatures, firewalls, virus protection, virtual private networks and encryption.[53]

2. GLB

The Financial Services Modernization Act of 1999, also known as the Gramm Leach Bliley Act (GLB), was enacted by the U.S. Congress and had a dramatic impact upon its inception.[54] Among other things, one of the relevant provisions of the GLB is to enhance data security among financial institutions and creditors.[55] Also known as the Safeguards Rule, the GLB requires companies to develop a written information security plan that describes how the company is prepared for and plans to continue to protect consumers' data, specifically, nonpublic personal information (NPI).[56] The purpose of such a security plan is to: (1) protect "the security and confidentiality of" the NPI; (2) "protect against anticipated threats or hazards to the security or integrity" of the NPI; and (3) "protect against unauthorized access to or

---

Common Law, 33 RUTGERS L.J. 617, 617 (2002).

49. 45 C.F.R. § 614.514(b)(2)(i) (2011).
50. *Id.* §§ 164.308-.314.
51. Kibbe, *supra* note 46, at 41-42.
52. *Id.* at 42.
53. *Id.* at 42-43.
54. *See* 15 U.S.C. §§ 6801-6809 (2006).
55. *Id.* § 6801.
56. *Id.* § 6803.

use of [the NPI that] could result in substantial harm or inconvenience to [the] consumer" who disclosed such NPI.[57] As part of this, the GLB specifically requires, among other things, that the company entrusted with the NPI: (1) assign at least one employee to manage the safeguards put in place to protect the NPI; (2) construct a thorough risk management plan on each department handling the NPI; (3) develop, monitor, and test a program to secure the NPI; and (4) change the safeguards as needed with the changes in how NPI is collected, stored, and used.[58]

3. FTC Red Flag Rules

While not a regulation per se, another U.S. law may further the responsibilities of cloud computing providers by attempting to create an environment of compliance and build trust in the United States. By implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, the U.S. Federal Trade Commission (FTC) issued the "Red Flag Rules" in 2008.[59] These require financial institutions and creditors to develop and implement written identity theft prevention programs that must provide for the identification, detection, and response to patterns, practices, or specific activities, known as "red flags," that could indicate identity theft.[60] One may ask that if their business practices conform to the HIPAA and GLB data security requirements, whether an additional program is necessary for compliance with the FTC Red Flag Rules. The answer is yes. Where the data security provisions of HIPAA and GLB leave off, the Red Flag Rules pick up.[61] One aspect of data security provisions is to *prevent* identity theft. However, the Red Flag Rules are designed to *recognize* identity theft in action.[62] Incorporating data security practices is one thing, but having an identity theft program in place is a different kind of plan, aspiring to manage a different stage of the misdeed.

Existing federal legislation regarding data security is, safe to say, lagging. As discussed later, there are more stringent state laws and even more stringent foreign laws. However, there have been attempts to create a new federal law to regulate data security in the United States. If

---

57. *Id.* § 6801(b).

58. 16 C.F.R. § 314.3-.4 (2011).

59. *New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft*, FED. TRADE COMM'N BUREAU OF CONSUMER PROT., 2008, http://www.alalm.org/PDF%20pages/State%20and%20Federal%20Regulations/Red%20Flag%20Overview2.pdf.

60. 16 C.F.R. § 681.1(d) (2011).

61. *The Red Flags Rule: Frequently Asked Questions*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm (last visited Sept. 29, 2011).

62. 16 C.F.R. § 681.1(d).

enacted, the new law(s) would again be something that cloud computing providers must follow to maintain the trust they hopefully built with their U.S. company customer. For instance, in May 2010, two U.S. House Representatives proposed new federal legislation that would create new protections for certain data.[63] "Covered information" which is collected and stored would be subject to an "opt-out" approach, while "sensitive information" would be subject to an "opt-in" approach.[64] In addition, another proposed law, the Data Accountability and Trust Act, would require companies that store personally identifiable information to implement security policies and procedures to ensure that information is adequately protected.[65] The good news for U.S. companies, and their entrusted cloud computing providers, is that these proposed laws largely match those requirements already covered by the GLB. Therefore, if currently in federal compliance, implementation of any of these proposed laws should not be a major issue for a cloud provider to continue to warrant and represent federal data security compliance.

B. *U.S. State Laws*

The second level of legal regulation regarding data security in the United States is ever-growing in popularity, but has three main laws already in place. The states of Maryland, Nevada and Massachusetts have data security obligations for companies that cloud computing providers must be aware of and comply with to continue building trust with their U.S. company customers. In comparison to the federal laws, the state laws can be viewed as a bit more stringent.

1. Maryland

The first is called the Maryland Personal Information Protection Act, enacted in 2008, and codified in the Maryland Code section 14–3503.[66] This Act mandates that companies who do business in the State of Maryland have certain obligations with respect to the "personal information" they receive from consumers in order to prevent identity

63. Mark McCreary, *New Effort at Federal Privacy Law Big on Promises*, PRIVACY COMPLIANCE & DATA SEC. (May 12, 2010, 9:39 AM), http://dataprivacy.foxrothschild.com/2010/05/articles/proposed-law/new-effort-at-federal-privacy-law-big-on-promises/.

64. *Id.*

65. Mark McCreary, *Data Accountability and Trust Act: Federal Breach Notification, Data Security Policies and File Access Addressed*, PRIVACY COMPLIANCE & DATA SEC. (May 7, 2009, 9:08 AM), http://dataprivacy.foxrothschild.com/2009/05/articles/proposed-law/data-accountability-and-trust-act-federal-breach-notification-data-security-policies-and-file-access-addressed/.

66. MD. CODE ANN., COM. LAW § 14-3503 (West 2011).

theft and other consumer harm.[67]

> [In order t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State [of Maryland] shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.[68]

Most notably for cloud computing providers, this law also requires that a company that uses a "nonaffiliated third party as a service provider" (read cloud computing providers) and discloses personal information about a Maryland resident under a written contract with that third party service provider, "shall require by contract that the third party implement and maintain reasonable security procedures and practices that: (i) [a]re appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and (ii) are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction."[69] While perhaps cumbersome, the requirement to "implement and maintain reasonable security procedures and practices" is not defined or elaborated upon.[70] Also, what is "reasonable" or "reasonably designed" can open up the conversation for a whole litany of practices that may protect personal information in different ways. However, being over-inclusive and going beyond "reasonable" is often the best practice as compliance is then practically ensured.

2. Nevada

In 2008, Nevada became the first State to enact law requiring the encryption for the transmission of certain personal information as defined in section 597.970 of the Nevada Revised Statutes.[71] While there are other state and federal regulations that certainly imply companies consider using encryption, no law in the United States required the encryption in the transmission of personal information prior to this Nevada law.[72] However, in 2009, the Nevada State legislature

67. *Id.* § 14-3503(a).
68. *Id.*
69. *Id.* § 14-3503(b)(1).
70. *Id.* § 14-3503(a).
71. NEV. REV. STAT. § 597.970 (2008) (repealed by 2009 NEV. STAT., c. 355, § 2).
72. Charlene Brownlee, *Nevada Passes First Law Requiring Business to Encrypt Customer Personal Information During Transmission*, PRIVACY & SEC. L. BLOG (Oct. 19, 2007), http://www.privsecblog.com/2007/10/articles/state-legislation/nevada-passes-first-law-requirin

repealed section 597.970, effective January 1, 2010.[73] But, in what can be seen as a certain bit of foreshadowing, the law took an approach to data security that may be enacted elsewhere in the future.

Thus, it is important to note the law and its requirements in the event of others borrowing its language for their own legislative use. While "personal information" is essentially afforded the same definition as other jurisdictions, as defined, "encryption" means a method "adopted by an established standards setting body, and which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data."[74] This makes the standards setting bodies more important in their influence. As a proactive measure, cloud computing providers are wise to implement the suggested encryption standards in that cloud provider's transmission of PII.

3. Massachusetts

Perhaps the most controversial and publicized state data security law is that in effect in Massachusetts. Enacted in 2008 and, much to the persuasion of U.S. companies buying time for the burdensome implementation, it was amended to take effect in 2010.[75] Massachusetts 201 CMR 17 affects all who own or license the personal data of a Massachusetts resident.[76] It establishes standards to be met in regards to safeguarding that personal data contained in either paper or electronic records.[77] The objective of this law is to ensure the security and confidentiality of the personal data by protecting it against anticipated threats or hazards, and unauthorized access or use.[78] Nearly all who have weighed in on this contentious law say that it will change the way companies store and transfer personal data. To begin with, it draws from other laws like HIPAA, GLB and the law in Maryland by requiring a comprehensive information security program combined with administrative, technical, and physical safeguards.[79] Many of the administrative and physical requirements are the same, such as designating an employee to operate, drafting security policies, imposing penalties, assessing risks and imposing physical personnel restrictions in certain areas.[80] However, rather than a blanket statement requiring

g-business-to-encrypt-customer-personal-information-during-transmission/.

73. S. 227, 2009 Leg., 75th Sess. (Nev. 2009).

74. NEV. REV. STAT. § 603A.215(b) (2010).

75. MASS. CODE REGS. § 17.00 (2011).

76. *Id.* § 17.01(2).

77. *Id.* § 17.01(1).

78. *Id.*

79. *Id.* § 17.03(1).

80. *Id.* § 17.03(2)(a)-(d).

"reasonable" practices or vague policies meant to keep the data secure as we have seen in Maryland (or even as it was in Nevada), Massachusetts has specific technical requirements that must be implemented when processing personal data. Like HIPAA, these include user authentication for secure access, monitoring of systems for unauthorized use, up-to-date firewall protection and the education and training of employees.[81]

One final technical safeguard, in addition to HIPAA, is the requirement for encryption of the data during transmissions as well as on portable devices.[82] This means that companies that have such data may be required to have all of their company laptops encrypted. In addition, and on a welcome note, encryption is not defined as it was in Nevada as necessitating compliance with standards, but rather includes the more generous definition of encryption as a "form in which meaning cannot be assigned without the use of a confidential process or key."[83] However, the most important aspect of this law for cloud computing providers is the third party service provider provision. Like Maryland, Massachusetts requires contractual provisions with third party service providers (read cloud computing providers) that maintain the effectiveness and maintenance of the law.[84] The company who possesses the personal data must select a third-party service provider that is capable of "maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations."[85] Also, the company must require by contract that such third-party service providers implement and maintain such appropriate security measures for personal data.[86] So, beyond the critical step of building trust, cloud computing providers are not just advised, but are indeed required to implement and maintain these security measures if they want to do business with certain U.S. companies.[87] Finally, it is apparent that this Massachusetts law has brought together many of the elements of its federal and state predecessors to compose the most comprehensive data security regulation for cloud providers.

C. *European Law*

Even with the list of U.S. laws and regulations that cloud computing

81. *Id.* § 17.04(1), (3), (4), (6), (8) (2011).
82. *Id.* § 17.04(3).
83. *Id.* § 17.02.
84. *Id.* § 17.03(f)(1).
85. *Id.*
86. *Id.* § 17.03(2)(f)(2).
87. *Id.*

providers must be comply with to earn the trust and business of U.S. companies, there are some foreign laws and regulations that must also be mentioned for the sake of furthering awareness and potential compliance. This is because the physical location of the cloud provider's servers may prohibit a U.S. company from doing business with them. For instance, the European Union has regulations on the management of certain data within its borders.[88] If a company entrusts the cloud computing provider with data of residents in this jurisdiction, then there may be certain restrictions on where the data can be sent and stored outside such a jurisdiction. Thus, if the cloud provider has servers located outside the European Union, and the U.S. company collects certain data from EU residents to be sent to the cloud provider, there may be an issue that the cloud provider must be aware of to accurately represent and warrant compliance with the foreign regulation. Also, it should be noted that the EU legislation is not exhaustive of all the global data security laws, it is just a snapshot of the predominant data security law most applicable to U.S. companies, given its broad scope.

Implemented by the European Commission in 1995, the EU Data Protection Directive 95/46/EC (EU Directive) broadly applies to twenty-seven countries in Europe. The purpose of the law is to protect "personal data" of EU residents.[89] Much like PII or other protected classes of data in the United States, "personal data" that is the subject of the EU Directive is loosely defined as "any information relating to an identified or identifiable natural person; an 'identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[90] As is evident, this definition, and the geographic scope of it, applies to a lot of data from a wide-range of potential people. Depending on the size of the U.S. company that the cloud computing provider does business with, there could be a good chance that the U.S. company has customers or employees in the European Union whose "personal data" fall under this EU Directive. It is the transfer of this data outside the European Union—and the EU Directives rules regarding such—that cloud providers must be conscious of when dealing with U.S. companies entrusting the cloud provider with this data. In this instance, such transfer outside the European Union (*i.e.*, the cloud providers' servers are outside the European Union), must be to a country that ensures an "adequate level of protection" for the subject data.[91] Loosely defined as "assessed in the light of all the circumstances," an adequate level of

88. *See* Council Directive 95/46, 1995 O.J. (L 281).
89. Council Directive 95/46, art. 1, 1995 O.J. (L 281) 1.
90. Council Directive 95/46, art. 2 1995 O.J. (L 281) a.
91. Council Directive 95/46, art. 25, 1995 O.J. (L 281) 1.

protection as further defined in Article 25(2) considers the nature of the data, the purpose and duration of the proposed transfer, and the rules of law in force in the receiving country.[92] Little guidance is given as to which countries ensure an adequate level of protection, thus cloud providers do not know where they can house servers and still comply with the EU Directive. However, there is hope using two practical possibilities if the cloud provider houses servers outside the European Union.

The first comes from the United States and the European Union having negotiated what is called the Safe Harbor Frameworks. These allow for a U.S. entity to certify implementation of certain data security requirements and thus be labeled by the European Union as ensuring an adequate level of protection.[93] Having all servers in the United States and warranting to the U.S. company customer that they are certified under the Safe Harbor framework is possibility number one for cloud computing providers. Another possibility comes directly from the EU Directive itself. Article 26 allows for the transfer of the subject data to a non-EU country under certain conditions.[94] A U.S. company, who has EU Directive subject data can transfer it to the cloud computing provider with servers outside the European Union if: (1) it gains the consent of the consumer (data subject); (2) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or (3) the transfer is necessary to protect the vital interests of the data subject.[95] However, the U.S. company must then only transfer the data to the cloud provider if it "adduces adequate safeguards with respect to the protection of the . . . [data]. . . ."[96] How is this done? Article 26(2) goes on to state that "such safeguards may in particular result from appropriate contractual clauses."[97] And there lies the cloud providers chance to earn trust. The cloud provider can transfer EU Directive subject data to servers outside the European Union if they represent and warrant via contract with the U.S. company that their servers—wherever they may be—utilize "adequate safeguards" within the meaning and scope of Article 25(2). Thus, there are two possibilities for cloud computing providers to overcome the hurdle of EU personal data protection laws; neither is impractical nor burdensome. Therefore, earning the trust of U.S. companies bound by this EU regulation should be easy for any serious cloud computing provider.

---

92. Council Directive 95/46, art. 25, 1995 O.J. (L 281) 2.

93. *Safe Harbor Privacy Principles*, DEP'T OF COMMERCE (July 21, 2010), http://export.gov/safeharbor/eu/eg_main_018475.asp.

94. Council Directive 95/46, art. 26, 1995 O.J. (L 281) 1.

95. Council Directive 95/46, art. 1, 1995 O.J. (L 281) 1(a), (b), (e).

96. Council Directive 95/46, art. 26, 1995 O.J. (L 281) 2.

97. *Id.*

The laws and regulations discussed above are not comprehensive of all the data security provisions governing the flow of data throughout the United States, or even the world. However, the most predominant and glaring of these are included herein. While compliance with these laws and regulations will require further research and internal assessments by each unique cloud provider, this Article shows that the idea and scope of compliance is within reach. Representing the majority of all data security concerns for U.S. companies, cloud computing providers can read and implement the above-mentioned laws and regulations to build a foundation upon which to build trust from U.S. companies they want to do business with.

V. CLOUD COMPUTING PROVIDERS BUILDING TRUST WITH U.S. COMPANIES

Laws and regulations carry penalties that no U.S. company wants to face when they are given data and obligated to implement certain security provisions to prevent the disclosure of such data. As the data owners will be giving their information to a U.S. company in confidence, such data owners are trusting that the company will keep their data secure. Trust becomes the ultimate factor—both on a consumer level and on a governmental level. If a company chooses to utilize a third party service provider (*i.e.*, a cloud provider) to process or store this data, then the company must be able to trust that the cloud provider will not disclose the data and that the cloud provider will adhere to the applicable U.S. laws and regulations. Trust that the data will be secure and regulations followed lets U.S. companies decrease their perceived risk of facing penalties, and even worse, the potential loss of reputation in the eyes of its consumers.

There are several ways and means in which a cloud computing provider can establish trust and gain the business of U.S. companies. Having certain policies in place and available for view by the U.S. company customer is one method that will be discussed later. Declaring past triumphs and current clientele is another. But the best method for a U.S. company to ensure that its interests are being upheld is to have a solid and comprehensive contract with the cloud computing provider. The contract between the U.S. company and the cloud computing provider can contain many different clauses that illuminate to the company that the cloud provider is serious about building trust. While this Article does not contain an exhaustive list of all contractual issues and provisions to include in any contract, it will donate a paragraph each to several contractual provisions a cloud computer can include in their contract with a U.S. company in order to build trust and gain

business.

The first and certainly the most important way to build trust via contract is to have the cloud computing provider represent and warrant compliance with all applicable data security laws and regulations. The contract will serve to govern the conditions upon which data is given to the cloud computing provider. The same data security provisions the company is subject to will in turn be incumbent on the cloud computing provider through written contractual clauses that the cloud provider must follow or be liable for breach of contract. While a data breach or non-compliance complaint event may be first directed at the company, if it occurred with respect to the data entrusted to the cloud provider, the company can then sue or otherwise demand their cloud computing provider to become liable for such data breach or non-compliance complaint event. Giving the U.S. company recourse for a data breach or non-compliance penalty allows the company to operate knowing it will not ultimately be liable. In addition, data breaches often come with a negative backlash in consumer sentiment. As such, the company can then have someone to point the finger at and absolve itself of some fault. Furthermore, and as discussed above, the laws and regulations incumbent on U.S. companies mandate similar security requirements and are mostly limited to certain PII-related data. Most of these requirements are already in place in larger companies, including large cloud providers. The data security requirements noted above are not uncommon or even difficult to implement. Thus, it is not impractical for cloud providers to represent and warrant compliance in a contract.

It can be said that performing an externally conducted risk assessment, and then being able to state in the contract the evidence and results of such, is not only necessary to build trust with customers, it ensures the cloud provider's own internal practices are legally secure. Contacting a local attorney or other third party specializing in data security laws is the best way for a cloud computing provider to show its seriousness in complying with all the applicable laws and regulations that it may be asked to represent and warrant in a contract with a U.S. company customer. While the cost of hiring an attorney to conduct research or a similar assessment may be high, the resulting new business and decrease in liability (assuming implementation of all the applicable data security provisions) will far outweigh the cost of a breach.

In November 2007, the United Kingdom launched a Privacy Impact Assessment process to help companies assess their operations for risk regarding data security.[98] Similar processes exist in Australia, Canada,

98. Pearson, *supra* note 16, § 5.1.

and the United States.[99] Mainly intended for use in the public sector, it can be of value to the private sector as well.[100] As the cloud computing industry grows, an array of these types of services may be offered to provide this assessment, especially as new and differing requirements in the level of data security required most certainly will be issued.[101] Receiving such assessments will further the commitment to data security that cloud computing providers can display to potential customers. Certainly, if there ever comes a governmental or standards body that can certify compliance with various laws and regulations regarding data security, this will immensely assist cloud providers in building trust by gaining such certificates.

Data breaches due to lack of data security is a topic close to all; the potential liability for U.S. companies in this event is vast. With regulatory fines and mandatory actions (*i.e.*, notification to affected consumers), a breach of data can bring devastating financial consequences. Consequential, indirect, and special damages are all present, along with actual direct damages in most all data breach cases. The loss of reputation, the cost of sending notifications to all affected consumers, the cost of damages that those consumers suffered, and the cost of implementing new and tighter security measures are all damages the cloud provider could contractually bind itself to. Assuming all financial obligations and damages of a data breach caused by the cloud provider gives the U.S. company customer no fear of a data breach and allows them to fully trust the cloud provider, it may indeed even enhance the business that transpires (due to the company being motivated to fully outsource data storage or processing because they can essentially outsource the ultimate liability too).

However, it is risky to agree to compensation for the loss of reputation due to the effectively inaccurate figure that could be proposed by the company. But, there are easily quantifiable figures that a company could calculate with respect to the cost of a data breach. In addition, cloud providers could sign up for liquidated damages in an amount stated in the contract. This saves the customer time in calculating damages post-breach and builds trust through a pre-determined amount of liability given. Contractually signing up to these damages may be overly burdensome, but they go a long ways in building trust and, indeed, technically give the liability to the appropriate owner (assuming the breach was the fault of the cloud provider).

Along those same lines, the non-monetary hassle a U.S. company

99. *Id.*
100. *Id.*
101. *Id.*

could face in the event of a breach could get ugly. Court battles and endless discovery relating to data breaches could drag a company down significantly. So to protect against these effects, a U.S. company customer will ask the cloud provider for indemnification from all lawsuits or other claims brought against the company relating to a data breach caused by the cloud provider. This, in essence, requires the cloud provider to step in the company's stead and assume all actions regarding such lawsuits or other claims—effectively leaving the company out of the picture. Like taking responsibility for the damages, indemnifying the U.S. company customer for all data breaches caused by the cloud provider is a contractual provision that most certainly will be required by the company.

However, there is some room for negotiation (and this too applies to the damages provision). The degree of care exercised by the cloud provider despite the breach need not be absolute. For instance, strict liability of any breach could be negotiated to a negligence or even a gross negligence level with respect to the degree of care provided by the cloud provider. This means that the cloud provider could try to negotiate terms in which they are not liable for a breach caused by them if they employed a certain level of protection or they acted in some negligent manner. A prudent cloud computing provider should be aware of strict liability clauses and their potential for negotiation into more reasonable or less assuming terms. However, in order to build the complete trust of the U.S. company, the cloud provider most likely must agree to full indemnification regardless of its level of care exercised.

Another contractual provision that a cloud provider could include in the contract to build trust is stating that it carries an insurance policy. Professional liability, acts and omissions, or even the newly founded data breach policies can show the U.S. company customer that the cloud computing provider has the ability to handle a breach of the data. This displays the financial resources to pay for the damages and indemnification discussed above. Most policies are inexpensive and should be considered a must for all cloud computing providers given the legal and financial exposure their business brings.

If a company is giving the cloud computing provider data, what happens then? The contract should state how the U.S. company customer can retrieve their data. If they want it back, that is a reasonable request since they should not face any undue factors delaying or denying a retrieval of data they own. The contract must state a certain number of days upon which the requested data will be returned by. Do not forget that under some laws, the data must be encrypted if it is transferred in any way. Thus, it may be advantageous to include in the contract the provision that the data is available at any time and will be encrypted. However, total destruction of the data raises another issue.

How and under what circumstances the data will be destroyed must be accurately reflected in the contract. The last thing a cloud provider wants to do is to destroy data that it either did not notify the customer of pending destruction or that the customer simply wants returned. Ensuring prompt return or effective destruction of data helps the cloud provider build trust with the customer who then knows that the data is available in the manner they choose.

Certain unlikely events that may occur in the contract lifecycle must also be addressed to build trust. If the cloud provider goes into bankruptcy, then the customer may want to know so that they can find another provider. In addition, the contract may stipulate how the data is to be returned in the event of a bankruptcy by the cloud provider. Also, if the cloud provider is subject to any merger or acquisition, then the customer may want to know that too, as the new company may not be one the customer wants to do business with. Contractual provisions that require prior written notice of these events are advised to be included in the contract. This allows the customer to trust the cloud provider because he will not all of a sudden find himself out of luck with no provider or find that he contracted to a non-desired company.

One final way to build trust contractually is through stating service levels. This requires the cloud computing provider to bestow upon the U.S. company customer certain levels of service that the cloud provider will adhere to or else face penalties to the company. One example is up-time. If the cloud provider states contractually that it will have a ninety-nine percent up-time (*i.e.*, their cloud services are available to the customer at least ninety-nine percent of the time), then it will be giving confidence to the customer that certain levels of up-time exist and the breach of such a provision will carry a penalty (also stated in the contract). Another service level that could be agreed upon is the functionality of the software service provided in the cloud. This functionality could be warranted to be free from bugs or other defects, or even that it will perform to certain specifications of the customer (although it is hard to warrant specific specifications unique to one customer as the cloud provider most likely has multiple customers). Most often, the service levels agreed upon will be found in an appendix or schedule to the main contract. Additional service levels may include software upgrades and other maintenance within certain frequencies. When U.S. company customers want to utilize a cloud computing provider, receiving contractual assurance that their user experience will be guaranteed to a certain level will provide them with trust that they will get what they are bargaining for, and if they get less, then they are contractually compensated for the lost balance.

Aside from using contractual provisions to build trust, there are other resources a cloud computing provider may turn to in its quest for

increased business with U.S. companies. One such resource is the idea of transparency. This means that the cloud provider gives data security and other applicable policies to the potential customer for review without redaction of pertinent items. These items include the different requirements under laws and regulations regarding data security, audit information, disaster recovery plans, or other essential items that the cloud provider can provide that relate to how a potential customer chooses a business partner (*i.e.*, codes of conduct, minority or women owned business status, or compliance with relevant law and regulations not related to data security). By openly displaying policies such as the cloud provider's data security regime, the potential customer can see the precautions and safeguards in effect and required by data security laws and regulations rather than just rely on the cloud provider's representation of compliance in the contract. Providing transparency can allow the U.S. company, as a potential customer, to declare even more due diligence in utilizing a cloud provider should any issues arise.

As mentioned above, disaster recovery plans are important. Having the cloud out of service is a serious event that may or may not have been preventable or even foreseen. The cloud provider can suffer these outages because of natural disasters, power failures, network errors or employee errors.[102] Each second the cloud is out, the cloud provider loses business from pay-as-you-go users, subscribers with service levels, and perhaps even worse, loss of reputation if the outage becomes widely known. However, a cloud provider having a disaster recovery plan not only ensures that they can resume business as quickly as possible after an outage, but it also signals to potential customers that the cloud is backed up by a plan to minimize down-time. Further assurance and trust-building of the disaster recovery plan's implementation is only as good as its ability to be carried out in real life. To this end, cloud providers should assure potential customers that they can be further trusted not only because a plan is in place, but because the necessary training of personnel has already taken place; thus, the provider is confident that all necessary steps are included in the plan.[103]

Given everything, there is one final block a cloud computing provider can use to build the foundation of trust. It is perhaps the most straight-forward manner in which to show a U.S. company that you can be trusted. Simply provide a spotless track record of no breaches, accompanied with positive testimonials of past and current customers. Testimonials that speak to the cloud computing provider's veracity and dependability certainly cast the cloud computing provider in a good

102. Mansfield-Devine, *supra* note 29, at 10.

103. *See* Virginia Cerullo & Michael J. Cerullo, *Business Continuity Planning: A Comprehensive Approach*, INFO. SYS. MGMT., Summer 2004, at 70.

light. The testimonials can be published on different websites (but most certainly on the cloud provider's website) or can be distributed to potential customers with sales material. Also, having a list of current customers available to potential customers is advantageous. It shows that others trust you with their data. The bigger the name and reputation of the customers on the list, perhaps the more the potential customer will be persuaded to trust and to engage in business with that cloud provider.

CONCLUSION

Cloud computing is certainly taking a foothold in the minds of companies across the world. Lower costs and convenience make cloud computing a great platform to perform many IT needs. However, this is a very young area of the IT industry. Comprehensive research and scrutiny have not yet been applied to present solid statistics or meaningful analysis. The rate of new laws and occurrences of data breaches in the United States remains a fluid figure that has no way of being predicted. However, what is known is that there are legal requirements in the United States regarding data security that U.S. companies must abide by to safeguard certain data given to them by consumers or employees.

Thus, the issue of data security in the cloud is—and unavoidably will remain—a major concern when choosing to utilize a cloud computing provider. Data breaches and the resulting loss of business and reputation are something that any company can simply not afford. If cloud computing is to become a viable solution, being able to trust the cloud computing provider to keep the data given to them secure is perhaps the most serious need for cloud providers to address when seeking business. Ensuring the integrity and security of the transmitted data entrusted to them means that cloud computing providers must have the appropriate security measures in place as dictated by relevant U.S. law. If a U.S. company is to utilize the cloud, the legal requirements must be contractually passed through to the cloud computing provider for the company to have control and recourse for potential liability in the case of a data breach. Then, trust can be built by the cloud computing provider by: (1) contractually representing to the customer that these legally required measures have been implemented; (2) applying the legally required measures to any data transmitted to them; and (3) accepting all liability for any breach or deficiency of such contractual representation. In addition, there are other ancillary methods in which trust can be built. Giving the customer as many of these factors as possible at the beginning of the relationship will ideally build a stronger

foundation of trust.

Because the downside can be potentially enormous, trust must be built in order for companies to tolerate the transmittal of data outside their confines. Cloud computing providers must be both vigilant in complying with all U.S. laws as well as concede contractual representations of such compliance and other protective measures. Only then can a U.S. company begin to build trust with the cloud computing provider and ultimately allow this new industry to grow as a legitimate option for U.S. customers.