Journal of Technology Law & Policy

Volume 16 | Issue 2 Article 1

December 2011

Chasing the Clouds Without Getting Drenched: A Call for Fair Practices in Cloud Computing Services

John Soma

Maury Nichols

Melodi Mosley Gates

Ana Gutiérrez

CHASING THE CLOUDS WITHOUT GETTING DRENCHED: A CALL FOR FAIR PRACTICES IN CLOUD COMPUTING SERVICES

John Soma,[*] *Maury Nichols,*[**] *Melodi Mosley Gates,*[***] & *Ana Gutiérrez*[****]

[*] John Soma is a professor of law at the University of Denver Sturm College of Law. Professor Soma is also the Executive Director of the University of Denver Privacy Foundation. After completing his Ph.D. in Economics in 1975, Soma served from 1976 to 1979 as trial attorney for the U.S. Department of Justice, Antitrust Division, Washington, D.C., where he was primarily assigned to the Department of Justice trial team in the United States v. IBM litigation. In 1979, he joined the University of Denver Sturm College of Law faculty. In addition to seven books on computer law, Soma has authored more than 40 professional articles in the computer law area.

[**] Maury Nichols holds a B.S. in Business Administration from Boston University (SMG '80) and a J.D. from University of Denver Sturm College of Law (2005). He is an active member of the Privacy Foundation Advisory Council. Maury is a Commercial Director at Capgemini US LLC. The opinions expressed by the author are those of the author and do not represent those of Capgemini.

[***] Melodi Mosley Gates holds a B.S. in Computer Science from California State University, Long Beach, a M.S. in Computer Science from the University of Colorado, and a J.D. from the University of Denver Sturm College of Law (Dec. 2010). With 20+ years experience in the information technology, she previously served as the Chief Information Security Officer for a large telecommunications organization. She is currently an Associate at Patton Boggs LLP in Denver, Colorado.

[****] Ana Gutiérrez holds a B.A. in Sociology and Spanish from Seattle University and a J.D. from the University of Denver Sturm College of Law. Gutiérrez was an Articles Editor on the *Denver University Law Review* from 2010-2011. Gutiérrez began working in the Environmental Regulatory Group at Hogan Lovells US LLP in Fall 2011. The opinions expressed by the author are those of the author and do not represent those of Hogan Lovells US LLP.

INTRODUCTION

With cloud services emerging as the latest computing technological advancement,[1] privacy looms as a critical component to the successful adoption of this technology. Through a comprehensive analysis of the looming dangers of privacy and security in clouds, this Article attempts to promote core principles and strategic business directions with the goal of fostering a consensus in legislative, regulatory, and international Internet policy. Influenced by the Federal Trade Commission's Privacy

[1] ANDY MULHOLLAND ET AL., ENTERPRISE CLOUD COMPUTING: A STRATEGY GUIDE FOR BUSINESS AND TECHNOLOGY LEADERS 15 (2010).

Initiative,[2] this Article advocates for the implementation of core privacy principles into cloud computing services. These core principles include facilitating transparency, empowering individuals to make informed and intelligent choices, strengthening multi-stakeholder governance models, promoting cooperation, and building trust in online environments.

Part I of this Article provides an overview of the historical and technical perspectives of cloud computing, and discusses its benefits. Part II addresses the inherent risks of cloud computing and demonstrates how the stage is set for the perfect storm to erupt if regulatory action does not take place. Part III introduces Carnegie Mellon's Software Engineering Institutes' Capability Maturity Model® Integration (CMMI^{SM})[3] as a way to project the development of privacy contracting principles within the cloud. This part also introduces five major business sectors to provide specific and distinguishable expectations for each business to evaluate its level of maturity. Finally, this part introduces the Federal Trade Commission (FTC) core privacy principles[4] as a guidepost for future regulatory action across all business industries.

Lastly, Part IV offers "shelter from the storm" by providing potential adopters of cloud services with suggestions to ensure that adequate protective controls are included as a part of their Service Level Agreement (SLA) negotiated with the provider. This Article concludes by making a call to implement the core FTC privacy principles into all "cloud" SLAs. Most of the private cloud sector's voluntary compliance with privacy regulation has been unsuccessful. Nonetheless, the cloud sector and interested investors should leverage these initial efforts to engage privacy regulation at the beginning of the maturity technological development stages to embrace core privacy principles across the industry and to optimize individual business prosperity.

I. CLEARING THE AIR: DISPELLING CONFUSION OVER THE BIG SKY OF CLOUD COMPUTING MODELS

Cloud-based computing involves the use of *Software as a Service*, *Platform as a Service*, and *Infrastructure as a Service*.[5] But, what does

[2] *See* FED. TRADE COMM'N, FAIR INFORMATION PRACTICE PRINCIPLES, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007) [hereinafter FAIR INFORMATION PRACTICE PRINCIPLES].

[3] SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON, CMMI FOR SYSTEMS ENGINEERING, SOFTWARE ENGINEERING, INTEGRATED PRODUCT AND PROCESS DEVELOPMENT, AND SUPPLIER SOURCING V 1.1, STAGED REPRESENTATION (2002), http://www.sei.cmu.edu/reports/02tr012.pdf [hereinafter SOFTWARE ENGINEERING INSTITUTE].

[4] *See* FAIR INFORMATION PRACTICE PRINCIPLES, *supra* note 2.

[5] PETER MELL & TIMOTHY GRANCE, U.S. DEP'T OF COM., SPECIAL PUB. 800-145

all of that mean? Unfortunately, the wave of the inexorable rush to the cloud has left a myriad of misinformation and market confusion. To clarify potential confusion about cloud computing, this part describes the historical development of the cloud, defines the cloud in practical terms, and defines the technological terminology. This discussion provides the necessary background to move beyond the technological schema of cloud computing and engages in a practical critique of the inherent privacy issues.

A. *Brief History of Cloud Computing*

While "cloud computing" is relatively new, the concepts inherent in cloud computing date from the 1960s.[6] When mainframe computers were extremely expensive to acquire, operate, and maintain, a number of firms decided to rent time to others on mainframe computers.[7] With the introduction of the relatively inexpensive mini-computer in the 1970s and the 1980s, the need to rent shared computing facilities faded into history.[8] During the 1990s, Application Service Providers (ASPs) became quite prevalent by providing standardized, fully-provisioned, and maintained applications that users could access over the Internet from their personal computer with a simple web browser.[9] While many of these providers vanished with the "dot.com" bust, their model was essentially the forerunner to today's Software as a Service cloud computing model.[10] With the advent of: (1) virtualization

(DRAFT), THE NIST DEFINITION OF CLOUD COMPUTING 2 *passim* (2011), http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

[6] MULHOLLAND ET AL., *supra* note 1, at 45.

[7] *Id.*

[8] *Id.*

[9]

> An *Application Service Provider ("ASP")* is a business that offers software services to customers, using computer networks and the Internet as the mechanism to deliver and manage the service. Among the most well-known Application Service Providers are Clickability, Salesforce.com and WebEx.
>
> The goal of an ASP business is to reduce the cost of software distribution and maintenance. Using a client/server model (often Web-based), network software can be installed in a centrally controlled place and *hosted*—accessed by the customers over remote links. This method to providing software solutions is sometimes called the software as a service ("SaaS") approach.

See Bradley Mitchell, *ASP—Application Service Provider*, ABOUT.COM, http://compnetworking.about.com/od/internetaccessproviders/g/providers_asp.htm (last visited Sept. 9, 2011).

[10] GREG SHIPLEY, INFORMATIONWEEK ANALYTICS, NAVIGATING THE STORM: GOVERNANCE, RISK AND COMPLIANCE IN THE CLOUD 10 (2009), http://reports.informationweek.com/

technologies;[11] (2) the ubiquitous deployment of the Internet; (3) the commoditization of hardware; as well as (4) the standardization of software, the stage was set for the re-emergence of a shared services computing architecture.[12] The current incarnation of this shared service model is now named cloud computing.

B. *Defining the Cloud*

Given that the cloud computing delivery model is relatively immature, there are many competing definitions which attempt to characterize this concept. For the purposes of this Article, the following broadly accepted definition, published by the National Institute of Standards and Technology (NIST), will be utilized: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[13] This Article focuses on exploring the implications of utilizing the various Service Models[14] and Deployment Models[15] defined by NIST in regulated environments.

1. The Three Service Models

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications while running operations on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (*e.g.*, web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

abstract/5/1075/Cloud-Computing/research-cloud-governance-risk-and-compliance.html.

[11] "Virtualization is a method of running multiple independent virtual operating systems on a single physical computer." George Ou, *Introduction to Server Virtualization*, TECH REPUBLIC (May 22, 2006), http://www.techrepublic.com/article/introduction-to-server-virtualization/6074941?tag=content;siu-container (discussing virtualization in depth).

[12] ACCENTURE, WHAT THE ENTERPRISE NEEDS TO KNOW ABOUT CLOUD COMPUTING 3 (2009), http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Technology_Labs_What_the_Enterprise_Needs_to_Know_About_Cloud_Computing.pdf.

[13] MELL & GRANCE, *supra* note 5, at 2. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. *Id.*

[14] *Id.*

[15] *Id.* at 3.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capabilities provided to the consumer are provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (*e.g.*, host firewalls).[16]

2. Deployment Models

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (*e.g.*, mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more cloud models (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (*e.g.*, cloud bursting for load balancing between clouds).[17]

C. *Analysis of Service Models*

In an IaaS Service Model, the user essentially has complete control

[16] *Id.* at 2-3.

[17] *Id.* at 3. Hybrid computing is a tiered computing approach that typically enables a user to retain control over the data in their data center (*e.g.*, security, back-up, retention, destruction, audit) while leveraging the elastic nature of a public cloud to perform bursts of processing on an as-needed basis. *Id.*

and responsibility regarding which applications will be deployed in the cloud.[18] As the cloud provider is simply renting computing and network resources to that user, the provider will typically only assume responsibility for the physical security of the environment and the availability of the infrastructure (*e.g.*, electricity, network connectivity, and server availability).[19] It is up to the user to implement appropriate application and database security mechanisms.[20] The user is also responsible for the security and regulatory compliance associated with the applications deployed in this model.[21]

At the other end of the risk-sharing spectrum is the SaaS model. With this Service Model, the cloud provider typically is responsible for both the infrastructure and the application.[22] The provider will therefore likely be responsible for both physical and logical security.[23] In addition, most SaaS providers will also offer the user SLAs related to the availability and response-time of the application; not just the underlying infrastructure.[24] Importantly, when the PaaS Service Model is utilized, the cloud provider will supply the user with the infrastructure mentioned in the IaaS model and the licenses to use the available software tools necessary for the user to develop and deploy applications.[25] Much like the IaaS model, the user is responsible for the application that is created and deployed in this environment.[26]

D. *Delivery Models*

Private clouds have gained the widest acceptance from users because the private cloud tends to allow the user to provision the most appropriate level of control and security.[27] Within a private cloud, only the user's company has access to the assigned computing environment.[28] This attribute significantly enhances the user's control of

[18] *Id.*

[19] CLOUD SEC. ALLIANCE, SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V 2.1, at 25 (Glenn Brunette & Rich Mogul eds., 2009), https://cloudsecurityalliance.org/csaguide.pdf [hereinafter SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V 2.1].

[20] *See id.* at 68-69.

[21] SHIPLEY, *supra* note 10, at 23.

[22] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V 2.1, *supra* note 19, at 25.

[23] *Id.*

[24] *Id.*

[25] SHIPLEY, *supra* note 10, at 9.

[26] *Id.*

[27] Jim Hietala, *Compliance Under a Cloud*, CIO (Feb. 24, 2010), http://www.cio.com/article/print/555163.

[28] MICHAEL BIDDICK, INFORMATIONWEEK ANALYTICS, GOVERNMENT CLOUD IMPLEMENTER'S CHECKLIST 8 (2010), http://i.cmpnet.com/infoweek/government/cloud/IWG_

the environment and materially reduces the risks associated with a multi-tenant environment; however, the user pays a premium for these features, as the costs cannot be shared with other tenants.[29] The "[c]ritical differentiators that private clouds offer over conventional data centers include on-demand IT [Information Technology] resources, usage-based metering, and 'elasticity,' or the ability to scale virtualized servers and storage up and down as needed."[30]

Community clouds represent a slight derivation from private clouds.[31] With a community cloud, multiple departments or agencies of the same entity share the computing environment.[32] This model offers some of the benefits of a multi-tenant environment while reducing risk by limiting those tenants to known entities.[33] Public clouds offer a user the least expensive access to computing resources.[34] A recent survey of public cloud providers found prices as low as 1.5 cents per Central Processing Unit (CPU) hour.[35] Given this very low price, there is an inherent tension within this model between balancing low-cost services with reasonable Service Level Agreements and reasonable availability metrics.[36]

Hybrid clouds enable a user to either retain a dedicated computing environment or a private cloud environment for their primary processing and then leverage the elastic nature of the public cloud for their over-flow processing, without relinquishing complete control to a public cloud.[37] For example, if a firm has provisioned their

Analytics_S1520810_CloudImplenter_Aug2010_final_final.pdf.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] ANDREW CONRY-MURRAY, INFORMATIONWEEK ANALYTICS, WHAT'S IN THE PUBLIC CLOUD 5 (2009), *available at* http://reports.informationweek.com/abstract/5/1152/Cloud-Computing/the-public-cloud-infrastructure-as-a-service.html.

[33] *Id.* at 6.

[34] *Id.* at 3.

[35] *Id.* As noted, CPU means Central Processing Unit, which is the part of the computer that performs calculations. Most non-virtualized computers are utilized about ten percent of the time. HYBRID HOSTING: EVOLVING THE CLOUD IN 2011, AMD 2 (2011), http://sites.amd.com/us/Documents/49701_Rackspace_Whitepaper.pdf. Therefore, in an average 60-minute "clock" hour, the CPU would have been used for six minutes. IaaS providers charge by the number of actual CPU hours used. *See Cloud Computing Billing Realities: IaaS Industry and Real Time Billing for Providers*, ARTICLESBASE (Sept. 9, 2011), http://www.articlesbase.com/software-articles/cloud-computing-billing-realities-iaas-industry-and-real-time-billing-for-iaas-providers-5202873.html. So, if a firm's usage of their in-house CPU is ten percent, this would indicate that they could run for approximately ten "clock" hours and consume one CPU hour.

[36] JONATHAN SHAW, CLOUD SERVICE NEGOTIATIONS: FIVE ESSENTIAL FACTORS (May 10, 2011), *available at* http://www.cioinsight.com/c/a/Bottom-Line/Cloud-Service-Negotiations-Five-Essential-Factors-411854/.

[37] David Linthicum, *What's the Deal with Private Clouds?*, INFORMATIONWEEK (Feb. 15, 2010, 10:27 PM), http://www.informationweek.com/news/cloud-computing/228901369.

infrastructure to meet their normal computing needs, but has cyclical or peak requirements for additional processing capacity, then leveraging a hybrid cloud model may be appropriate. Specifically, a firm that processes tax returns throughout the year, but encounters a significant spike in activity during the month of April might be a good candidate for using a hybrid cloud. In this case, that firm could engage the services of a public cloud provider to meet their over-flow processing requirements as opposed to procuring additional hardware to meet their peak processing requirements. This type of occasional usage of extra computer capacity in the cloud has become known as "cloud bursting."[38]

E. *Benefits of Utilizing a Cloud Computing Environment*

Businesses are beginning to experiment with cloud computing as this delivery model provides a number of appealing characteristics including: reduced cost, pricing flexibility, agility, and risk-reduction.[39] First, cloud computing facilities offer significantly improved utilization of computing resources by typically sharing resources across a number of users.[40] Individual companies have not been able to achieve reasonable utilization levels, primarily due to historical deployment methodologies.[41] Given the instability of early mid-range computing systems and their immature operating systems, most businesses tended to deploy a single application on one or more servers to reduce the risk of conflicts of executing multiple applications on the same server.[42] This deployment approach severely underutilizes server capacity[43] resulting in huge (and mostly unnecessary) financial costs for maintenance, licensing, and floor-space.[44] In fact, one study noted that on average only 6% of deployed serve capacity is actually used.[45] Cloud computing offers a flexible and scalable environment;[46] a cloud

[38] *Id.*

[39] *See* Emily Maltby, *Small Companies Look to Cloud for Savings in 2011*, WALL ST. J. (Dec. 29, 2010), *available at* http://online.wsj.com/article/SB10001424052970203513204576047972349898048.html?mod=outsidein&utm_source=twitterfeed&utm_medium=twitter.

[40] *Id.*

[41] CAPGEMINI, AN EARLY VIEW OF CLOUD COMPUTING 5 (2009), *available at* http://www.capgemini.com/insights-and-resources/by-publication/an_early_view_of_cloud_computing.

[42] *Id.* at 3 (noting that cloud computing can now support the resizing and reshaping of applications).

[43] *Id.* at 5.

[44] *Id.* at 6.

[45] MULHOLLAND ET AL., *supra* note 1, at 50.

[46] Neil Roiter, *How to Secure Cloud Computing*, INFO. SEC. MAG. (Mar. 9, 2010), http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349670,00.html.

computing vendor is able to offer a lower price to a user based upon the vendor's ability to obtain a higher level of utilization of the computing environment.[47]

Second, this more flexible environment enables a business to shift from a fixed cost structure to a variable cost structure, in turn, enabling a "pay for use" model.[48] In addition, many firms are able to treat these variable costs as an operating expense as opposed to a capital expense.[49] This accounting treatment may enable a firm to receive the necessary approvals to deploy a new application in less time, resulting in a faster time-to-market, which may lead to a competitive advantage.[50]

Third, utilization of a cloud environment enables a firm greater freedom to experiment with new applications by reducing their risk of failure. In a traditional, dedicated computing environment, a firm would need to justify the capital expenses related to acquiring and amortizing the necessary servers for a given application. If a particular application fails, the firm would likely have significant stranded costs. In a cloud computing environment, however, if the application fails, the firm would simply terminate the usage of that application without incurring stranded costs.

Fourth, enterprises typically provision their computing environment to handle peak processing loads.[51] This approach leads to significant under-utilization during non-peak processing times.[52] The idle servers still continue to consume electricity and typically require air conditioning. This wasted energy could be eliminated, and thus contribute to a "greener" IT environment, if the firm performed its processing on more fully-utilized servers housed within a shared services cloud computing environment.[53]

Fifth, utilizing cloud computing enables firms to reduce the time required to provision computing resources from months to minutes.[54] This reduced provisioning time has a number of benefits including: (1) reducing the time required to introduce new innovations; (2) cost savings in the deployment of computing environments; (3) reduced cost due to reductions in human error in configuring the environment; and

[47] *Id.*

[48] *Id.*

[49] SYMANTEC CORP., MITIGATING SECURITY RISK IN THE CLOUD 2 (2010), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-mitigating_security_risk_in_the_cloud_WP.en-us.pdf.

[50] *See id.*

[51] CAPGEMINI, *supra* note 41, at 6.

[52] *Id.* at 5.

[53] *Id.* at 6.

[54] IBM, SEEDING THE CLOUDS: KEY INFRASTRUCTURE ELEMENTS FOR CLOUD COMPUTING 4 (2009), http://www-935.ibm.com/services/in/cio/pdf/oiw03022usen.pdf.

(4) cost reduction through reuse of existing resources.[55]

Finally, many companies are not able to attract, retain, or (in some cases) afford the specialized personnel to protect their computing environment from the ever increasingly sophisticated Internet-based security threats. When a firm elects to utilize cloud computing, the provider typically has the ability to employ the appropriate resources to monitor, manage, and respond to these ever-evolving threats in a more efficient and cost-effective manner.[56] Cloud computing enables a company not only to share computing resources, but also to share the skills of highly trained and specialized personnel.

II. WHERE'S MY UMBRELLA? CLOUD COMPUTING RISKS & THE PERFECT STORM

Despite the level of hype surrounding cloud computing and the technology's immaturity, adoption levels continue to increase. A recent survey found that 60% of U.S. Chief Information Officers (CIOs) and a near majority of their European counterparts are pursuing a cloud computing approach due to the promise of lower costs and other business benefits.[57] Other studies show that even ambitious adoption estimates have now been surpassed.[58] This rapid cloud adoption, coupled with still evolving practices in risk management, creates an inevitable clash between the business leaders who long for operational flexibility and cost savings, and the risk managers who fret over loss of control and protection of information assets.[59] Moreover, smaller businesses and less-sophisticated IT consumers may not even recognize the tradeoffs to be weighed, but simply focus on the promise of being able to use IT services previously available only to those with large capital budgets and significant IT expertise.

[55] *Id.* at 5.

[56] FRAN HOWARTH, BLOOR RESEARCH, THE REALITIES OF WEB SECURITY 1, 4 (2010), *available at* http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1503957.

[57] CHRIS NUTTALL & KEN ADLER, PA CONSULTING GROUP & LOEB & LOEB LLP, MANAGING TURBULENCE IN THE CLOUD 1 (2010), *available at* http://www.loeb.com/managing turbulenceinthecloud/.

[58] Amy Newman, *Did Cloud Computing Jump the Shark?*, SERVERWATCH (Oct. 20, 2010), http://www.serverwatch.com/virtualization/article.php/3909231/Did-Cloud-Computing-Jump-the-Shark.htm; *see also* Sreedhar Kajeepeta, *Cloud Computing Adoption Rate Speeding Along*, CSC (Apr. 27, 2010), http://a6.64.354a.static.theplanet.com/cloud-computing-adoption-rate-speeding-along (noting that cloud adoption is going faster than industry analysts previously predicted).

[59] Mike Fratto, *Cloud Control*, INFORMATIONWEEK REPORTS 31-32 (Jan. 26, 2009), *available at* http://analytics.informationweek.com/abstract/22/729/soa-and-app-architecture/internet-evolution-cloud-control.html.

A. *Risks in an Uncertain World*

Industry experts remind those considering adoption of cloud services that, "leveraging the benefits of cloud and maintaining compliance can be at odds with each other."[60] Further, potential cloud services consumers must also consider the maturity level of the service provider, because an immature services provider is less likely to have the control processes in place that are so necessary for proper risk management. Six core areas of risk, common to all information system implementations, are identified in this part. The special issues raised by cloud computing services are also discussed: (1) privacy; (2) security; (3) business continuity; (4) records management; (5) interoperability; and (6) auditability. These risk areas frequently overlap, and dependencies are not uncommon; consequently, each risk must be considered in the broader environment and context of cloud services.[61]

1. Privacy

Cloud services consumers often create, store, transmit, or otherwise manage Personally Identifiable Information (PII), and other highly sensitive data as a part of their business and service offerings. Any business that accepts a credit card or electronic funds transfer as payment, for example, has access to sensitive personal financial information and is likely subject to special data protection obligations.[62] Healthcare providers may utilize cloud services to handle Protected Health Information (PHI),[63] while other organizations, including

[60] Chenxi Wang et al., *Compliance with Clouds: Caveat Emptor*, FORRESTER RESEARCH (Aug. 26, 2010), http://www.forrester.com/rb/Research/compliance_with_clouds_caveat_emptor/q/id/56690/t/2 (Executive Summary); *see also Q&A: Forrester's Chenxi Wang Discusses Cloud Compliance*, SEARCHCLOUDSECURITY.COM (Sept. 24, 2010), http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1520722,00.html?track=NL-430&ad=790304&asrc=EM_NLT_ 12627152&uid=10415695.

[61] For instance, as one learned colleague opined, "you can have security without privacy, but you cannot have privacy without security." Kevin Beaver, *Security and Compliance Can Go Together, When Done in the Right Order*, SEARCHCOMPLIANCE.COM (Sept. 2009), http://searchcompliance.techtarget.com/tip/Security-and-compliance-can-go-together-when-done-in-the-right-order. One of the authors had the good fortune to work for several years with Andy Holleman, Chief Privacy Officer, who often pointed out the need for strong security practices if one is to provide reliable, robust privacy protection for personal information.

[62] *See, e.g.*, PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS V 2.0, at 5 (2010), *available at* https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf.

[63] "Protected health information" or "PHI" and rules for its protection are defined in the rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). *See* Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections 45 C.F.R.).

employers and tax advisors, may use cloud services to handle social security numbers, driver's license numbers and other PII. In each of these cases, the cloud services consumer has downstream customers who expect their personal information to be protected and used only for the purposes they intend, as well as a variety of regulatory obligations.[64]

In considering appropriate privacy measures and practices, longstanding, widely accepted privacy principles, including those from the Organization for Economic Co-Operation and Development (OECD), are instructive. The OECD has established eight principles for PII data collection, handling, and privacy assurance: (1) Collection Limitation; (2) Data Quality; (3) Purpose Specification; (4) Use Limitation; (5) Security Safeguards; (6) Openness; (7) Individual Participation; and (8) Accountability.[65] Similarly, the Generally Accepted Privacy Principles (GAPP), maintained by the American Institute of CPAs, take a business perspective on an entity's responsibility in managing PII, and define ten principles that also include monitoring and enforcement of the organization's policy.[66] Finally, the FTC has adopted "five core principles of privacy protection" as its "Fair Information Practice Principles:" (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress.[67]

Privacy risks in information systems, including cloud computing environments, may be minimized by close adherence to these principles by both the services provider and consumer. Cloud services consumers must first identify and classify the sensitive data they plan to use in the cloud environment, and then ensure that their service provider takes a reasonable approach, based on accepted privacy and security principles. Privacy issues specific to cloud computing services have also recently gained FTC attention.[68]

[64] Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have passed data breach notification statutes that apply to personally-identifiable information such as social security numbers, financial accounts, driver's license numbers, and the like. *See generally State Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last updated Oct. 12, 2010).

[65] OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 14–16 (2001).

[66] AM. INST. OF CPAS, AN EXECUTIVE OVERVIEW OF GAPP: GENERALLY ACCEPTED PRIVACY PRINCIPLES 6 (2009), *available at* http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx.

[67] FAIR INFORMATION PRACTICE PRINCIPLES, *supra* note 2.

[68] *See* FED. TRADE COMM'N, THE FTC IN 2010: FEDERAL TRADE COMMISSION ANNUAL REPORT 40 (2010), http://www.ftc.gov/os/2010/04/2010Chairmans Report.pdf [hereinafter THE FTC IN 2010: FEDERAL TRADE COMMISSION ANNUAL REPORT]. The commission specifically included cloud computing—along with social networking and other emerging technologies—in

While the traditional privacy principles are useful, they are also somewhat abstract. One commentator has suggested that clarity around privacy issues in cloud computing may be best gained by both consumers and providers taking responsibility, and simplifying the discussion of cloud-based data exposure into three basic scenarios: (1) unintentional user-driven data leaks; (2) lack of controls or protections from the cloud provider; and (3) intentional data leaks for monetary gain.[69] The inherent centralization of the cloud services deployment model creates a high-value target for hackers and would-be identity thieves. Regardless of the approach taken, cloud providers and consumers must engage in an open dialogue and shared risk analysis to ensure privacy protection for downstream consumers.

2. Security

Security in information systems is typically defined as the countermeasures, or controls, employed to protect the confidentiality, integrity, and availability of the system.[70] Experts at the NIST describe cloud security as a "tractable problem" and note that cloud computing models offer advantages over more traditional distributed computing models, including simplified auditing and automated management, along with redundancy and disaster recovery capabilities.[71] Verifying the security controls implemented in a cloud services environment is paramount to the cloud services consumer, because using these services, especially in the SaaS model, requires the consumer to give up control of its information to the provider.[72]

its "Exploring Privacy Roundtables" sessions as described in its 2010 annual report. *Id.*

[69] Diana Kelley, *Rethinking Privacy and Cloud Computing*, ESECURITY PLANET (Nov. 1, 2010), http://www.esecurityplanet.com/article.php/3910876/Rethinking-Privacy-and-Cloud-Computing.htm.

[70] NAT'L INST. OF STANDARDS AND TECHS., U.S. DEP'T OF COM. SPECIAL PUB. 800-53, REV. 3, RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS 1 (2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[71] PETER MELL & TIM GRANCE, NIST INFO. TECH. LAB., EFFECTIVELY AND SECURELY USING THE CLOUD COMPUTING PARADIGM, 18-19 (2009), csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt (PowerPoint presentation).

[72] Recently, the White House's CIO Council has proposed a set of "baseline security requirements" for government sector adopters of cloud computing services, as a product of the Federal Risk and Authorization Management Program (FedRAMP). *See* CIO COUNCIL, PROPOSED SECURITY ASSESSMENT & AUTHORIZATION FOR U.S. GOVERNMENT CLOUD COMPUTING DRAFT VERSION 0.96, at 2-34 (2010), https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf. While comprehensive in their coverage, the detailed nature of the seventeen "baseline" requirements, based on the Federal Information Security Management Act (FISMA) and NIST guidance, may be too overwhelming for immediate adoption as by the private sector, especially by smaller or less

Those contemplating the use of cloud services are best positioned to understand their information assets and specific protection requirements. Thus, it will also be helpful for cloud clients to consider security issues in terms of the most common threats, especially those unique to cloud computing. The Cloud Security Alliance has identified seven "top threats" to cloud computing: (1) abuse and nefarious use of cloud computing; (2) insecure application programming interfaces; (3) malicious insiders; (4) shared technology vulnerabilities; (5) data loss/leakage; (6) account, service, and traffic hijacking; and (7) unknown risk profile.[73]

The unknown risk profile may be the most difficult threat for less sophisticated users to recognize and address, as it results from a lack of consumer knowledge regarding the cloud provider's services and the risks inherent to its infrastructure.[74] Cloud services consumers cannot simply acquiesce to the security practices of their cloud services provider, but instead must engage in reasonable diligence to ensure the provider's security controls are appropriate based on the sensitivity of the data managed.

3. Business Continuity

Those contemplating the use of cloud computing services must also consider their business continuity requirements and willingness to accept any disruption in services. The issue is not simply one of what technologies the cloud services provider utilizes and the availability of levels offered, but also financial and operational viability. As the user is almost totally dependent on the cloud, each cloud user must ask, "[w]hat if the vendor does not exist tomorrow?"[75]

While astute cloud service consumers will look for reliable service providers that are financially and operationally sound, it is also important that consumers match the cloud services they select with their business continuity needs. Moreover, the maturity levels of both the cloud services provider and consumer must be considered, especially since a less mature service provider may not have evolved its processes sufficiently to provide rapid, reliable recovery.[76] Similarly, a less mature consumer will have a greater dependency on its service provider

sophisticated cloud services consumers.

[73] CLOUD SEC. ALLIANCE, TOP THREATS TO CLOUD COMPUTING V 1.0, at 8-14 (2010), *available at* http://www.cloudsecurityalliance.org/topthreats.

[74] *Id.* at 7, 14.

[75] Vasant Raval, *Risk Landscape of Cloud Computing*, 1 ISACA J. 4 (2010), *available at* http://www.infotex.com/portal_blog/white_papers/risk_landscape_of_cloud_computing_isaca.pdf.

[76] *See Maturity of Cloud Computing*, *infra* Part V.A.

for sounds processes. The most troubling case occurs when both the provider and the consumer are still operating at lower maturity levels. A service offering which makes no promise of continued availability could be fatal to a data-driven small business such as an accounting or law firm that simply cannot function if its data is not available for days at a time.

Business continuity issues are most often considered in negative terms, that is, how to ensure the availability (or lack thereof) of the services does not impede the organization's ability to do business. While such considerations are true in the cloud services environment, the use of cloud services can also be viewed from a positive perspective for business continuity purposes. Cloud services that provide geographic distribution of resources and always-available services may facilitate business continuity planning and lower costs over more traditional methods.[77] As with other risks, the critical factor for the cloud services consumer is to understand its requirements and ensure that the SLA offered by the cloud services provider is a good fit.

4. Records Management

Records management issues, including ready access to and searching of stored information, archiving, planned records destruction, and e-discovery capabilities are critical to many businesses, especially for those with specific retention obligations under the Sarbanes-Oxley Act and other laws.[78] Records management and ready access to data is also an issue for any business or other organization that may be subject to litigation, because the Federal Rules of Civil Procedure now require litigants to retain electronic records in the anticipation of litigation.[79] Finally, consumers must be careful to retain data ownership and access in the event either party terminates their cloud services agreement. Cloud computing consumers must always remain aware of their obligations and scrutinize service offerings to ensure records are maintained in an acceptable manner.

Consumers may also need to consider compensating controls or additional, layered services to ensure their records management obligations are met. The National Archive and Records Administration has, for example, advised federal agencies about data retention and records relating to cloud computing, noting in particular, that cloud service providers should be closely scrutinized because they may not

[77] Chris Pyle, *How to Ensure Business Continuity with Cloud Computing*, EWEEK.COM (July 7, 2010), http://www.eweek.com/c/a/Cloud-Computing/How-to-Ensure-Business-Continuity-with-Cloud-Computing/.

[78] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745.

[79] FED. R. CIV. P. 26(a)(1)(A), 26(b)(1)(B) (2006).

sufficiently address specific records retention requirements.[80]

5. Interoperability

While not necessarily a risk to the cloud consumer's current data, interoperability capabilities (or lack of) may create a business risk by limiting the consumer's flexibility in moving to another service, adding new functions, or otherwise engaging in innovation. Data sharing and integration mechanisms are key to realizing the full value of cloud computing, especially among collaborating organizations that may use different service providers.[81] Businesses especially need interoperability between their existing, in-house infrastructure and cloud-based services, as well as the ability to move from one cloud provider to another without incurring substantial transition costs.[82]

Unfortunately, in today's fast-evolving cloud services market, sufficient incentives do not yet exist for vendors to cooperate and provide interoperability.[83] Cloud services consumers must carefully review and plan their data migration paths and continue to pressure service providers to adopt standard data sharing and integration mechanisms as they mature.

6. Auditability

Cloud services consumers often find themselves in a position of needing to provide assurances regarding their computing environment to regulators, their downstream customers, or both. Traditional, in-house computing models made meeting these audit requirements fairly straightforward since the organization was in control of its own computing platforms. With cloud computing services, it may be difficult, or even contrary to the services agreement, to perform a formal audit on the computing environment. Service providers often provide a

[80] *Frequently Asked Questions About Managing Federal Records in Cloud Computing Environments*, U.S. NAT'L ARCHIVES AND RECS. ADMIN., http://www.archives.gov/records-mgmt/faqs/cloud.html (last visited Sept. 27, 2011); *see also* Elizabeth Montalbano, *NARA Addresses Cloud Record Keeping*, INFORMATIONWEEK GOVERNMENT (Feb. 22, 2010, 11:50 AM), http://www.informationweek.com/news/government/info-management/showArticle.jhtml?articleID=223100117.

[81] David Linthicum, *The Data Interoperability Challenge for Cloud Computing*, INFOWORLD (Jan. 12, 2010, 4:00 AM), http://www.infoworld.com/d/cloud-computing/data-interoperability-challenge-cloud-computing-259.

[82] George Lawton, *Addressing the Challenge of Cloud-Computing Interoperability*, COMPUTING NOW (2009), http://www.computer.org/portal/web/computingnow/archive/news031.

[83] *Id.*

SAS-70[84] audit statement to their customers, but these statements may be limited in their content and insufficient to satisfy an organization's need for comprehensive risk analysis. Moreover, the consumer must carefully scrutinize the provider's auditing method and the independence of the auditors involved before relying on its findings. In an effort to address these perceived shortcomings, the American Institute of CPAs is in the process of transitioning the SAS-70 auditing standard to a series of Service Organization Control (SOC) Reports standards, but that migration will take time.[85]

More sophisticated consumers, including large enterprises with their own IT governance resources, may look to performing their own reviews using a widely accepted IT governance framework that ensures all common control requirements are met.[86] But even these more resource-rich organizations are likely to encounter resistance from their service providers. Without standard disclosures, this risk offers perhaps the strongest reminder of "caveat emptor" for the cloud services consumer, since the other risks, as described above, can only be properly recognized and effectively mitigated by reliable auditing processes.

B. *The Perfect Storm*

Cloud computing consumers' lack of control over their information and computing environments creates a series of business risks. Further, those risks may be difficult to quantify without reliable, independent auditing. A loss of information, or even a prolonged lack of access may bankrupt a data-intensive business in today's competitive environment. This situation is further compounded by the default terms and conditions common in today's cloud services agreements that must be closely scrutinized, understood, and appropriately negotiated to avoid[87]

[84] *See SAS 70 Service Organization Auditing Standards*, SAS 70, http://www.sas70.com (last visited Sept. 27, 2011). A SAS-70 audit provides a third party assurance concerning the implementation, ongoing maintenance, and effectiveness of controls within service provider environments (*e.g.*, security, business continuity). The service provider typically defines the controls themselves and the scope of the audit, thus a caveat emptor and a detailed review of the audit report is needed. *SAS 70's* FAQs, SAS 70, http://sas70.com/sas70_faqs.html (last visited Sept. 27, 2011). For example, there is no preset standard for controls that must be met to "comply with SAS-70." *Id.*

[85] *See* "Service Organization Controls Reports," American Institute of CPAs, http:// www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx (last visited Oct. 16, 2011).

[86] For example "COBIT," Control Objectives for IT, from the Information Systems Audit and Control Association (ISACA). *See COBIT Framework for IT Governance and Control*, ISACA, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx (last visited Sept. 27, 2011).

[87] Edward A. Pisacreta, *A Checklist for Cloud Computing Deals*, L. TECH. NEWS (Apr. 9,

a perfect storm of business risk and lack of accountability from raining down on unwary or unprepared consumers.

For example, Amazon Web Services' public cloud terms and conditions address the following concepts: (1) the consumer must acknowledge that Amazon may suspend access at any time, may revise the agreement at any time, and the consumer agrees to abide by any such revisions; (2) that the provider is not liable for any unauthorized use or other security breach; and (3) the provider may terminate the services for any reason with 30 days notice.[88] Amazon also limits the consumer's ability to use open source software that is commonly utilized to lower deployment costs and simplify maintenance.[89] Similarly, Google states in its terms that because it is "constantly innovating in order to provide the best possible experience for its users," it may change the services it provides at any time, without prior notice, and that it is not liable for any damages incurred by users due to such changes.[90]

Given their size and bargaining power, cloud services providers are in a position to dictate terms that are favorable to themselves, but risky for consumers. In their current forms, these agreements could be termed adhesion contracts, and unsophisticated consumers may not even recognize the risk they are taking, including the complete loss of the services they have used to build their businesses. While cloud service providers may have a legitimate argument that they can only provide cost-effective services with standardized agreements that limit their liability, some further protection for consumers is needed, especially for those less aware of the risks. At a minimum, the user should seek to acquire cloud computing services from a provider that offers reasonable SLAs to compensate them in the event of a service level failure.

V. FORECAST: SCATTERED LEGAL SHOWERS, HEAVY IN SOME PRIVACY AREAS

One of the most important advantages of cloud computing is that it is a dynamic infrastructure. The flexibility inherent in cloud computing permits accessibility to multiple data centers worldwide, allows businesses to access their systems remotely if need be, and

2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202447767770&slreturn=1&hbxlogin=1.

[88] *AWS Customer Agreement*, AMAZON WEB SERVICES, http://aws.amazon.com/agreement/ (last updated Aug. 23, 2011).

[89] *Id.*

[90] *Google Terms of Service*, GOOGLE (Apr. 16, 2007), http://www.google.com/ accounts/ TOS.

exponentially increases the amount of data that can be stored and processed in the cloud. So, what are the negatives? Cloud computing is a relatively novel concept with little legal or regulatory infrastructure. As a result of the rapid adoption of these new cloud systems coupled with the current lack of standards and regulations to govern best practices and fair bargains, businesses and consumers may be at serious risk, and they may not even realize it. This is particularly true for unsophisticated businesses, but it is also applicable to sophisticated entities that lack bargaining power or simply do not have the requisite knowledge to negotiate specific contract terms that will best protect their business.

There are certain privacy and security concerns and regulatory obligations that businesses should take into consideration when deciding whether to use cloud computing as an integral system of data storage and organization. How do you ensure that your data is secure and private? Who has access to the encryption keys? Can you efficiently migrate data? How will the data be disposed of upon termination of the contract? What terms should be included in the contract to effectively protect the business? Does the service provider understand the pertinent regulations and provide compliance support? Who will audit the service provider? This part focuses on these questions by dissecting the theoretical concepts of cloud computing and analyzing the contractual terms necessary to protect businesses of all sizes and across various industries that are engaged in or converting to cloud computing.

Naturally, the analysis for each business must be on a case-by-case basis. The goal is to protect consumers and businesses alike by establishing a set of understandable and core privacy "best practices." Cloud computing has the potential to be an extremely valuable asset for businesses and industries. However, the disadvantages, including the lack of fair information practices in cloud computing services, the serious risks of deficient privacy and security, as well as the need for mature business continuity, records management, and interoperability support, simply may not outweigh the clouds' benefits.

In order to reach their ideal level of information technology, including cloud infrastructure and maturity, businesses should look to the Carnegie Mellon's Software Engineering Institutes' Capability Maturity Model® Integration (CMMI^{SM}) system.[91] At each stage, the core FTC privacy principles should be used.

This part begins by providing an overview and explanation of the CMMI process improvement approach to attaining a business's ideal level of IT maturity. Next, because a business's size, nature, and industry will invariably form the content of a negotiated contract, this part

[91] SOFTWARE ENGINEERING INSTITUTE, *supra* note 3, at 11.

introduces five major business sectors which provide specific and distinguishable expectations and federal regulatory compliance issues for each business to evaluate its level of maturity. Finally, this part introduces the FTC core privacy principles as a guidepost for future regulatory action across all business industries.

A. *Maturity of Cloud Computing*

One common way to analyze the maturity of an organization's IT infrastructure and supporting processes is the Carnegie Mellon's Software Engineering Institutes' Capability Maturity Model® Integration (CMMI^{SM}).[92] The CMMI model broadly defines five maturity phases:

(1) Initial: At this beginning maturity level, "processes are usually *ad hoc* and chaotic. The organization usually does not provide a stable environment. Success depends on the competence and heroics of the people in the organization and not on the use of proven processes."[93]

(2) Repeatable: At this stage, "[c]ommitments are established among relevant stakeholders and are revised as needed. Work products are reviewed with stakeholders and are controlled. The work products and services also satisfy their specified requirements, standards, and objectives."[94]

(3) Defined: At this maturity stage, "processes are well-characterized and understood, and are described in standards, procedures, tools, and methods. . . . [T]he standards, process descriptions, and procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit."[95]

(4) Managed: "Quantitative objectives for quality and process performance are established and used as criteria in managing processes. . . . [T]he needs of the customer, end users, organization, and process implementers are established. Quality and process performances are understood in statistical terms and are managed throughout the life of the processes."[96]

(5) Optimizing: Here, the focus is on "continually improving process

[92] *Id.*

[93] *Id.* at 11-13.

[94] *Id.*

[95] *Id.*

[96] *Id.*

performance through both incremental and innovative technological improvements. Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement."[97]

Based upon the CMMI criteria, the maturity of cloud computing may vary by the specific Deployment Model (*e.g.*, private, community, public, or hybrid) and to some extent by the selected Service Model (*i.e.*, SaaS, PaaS, and IaaS).[98] Unlike mature software development and integration organizations, cloud services providers are still evolving their service delivery models and they frequently offer little in terms of transparency.[99]

Many seasoned computer industry observers believe that cloud computing is a decade behind the Internet and is "wild, wooly, full of promise and hype, and constantly changing."[100] Other industry experts observe, "that security is the biggest barrier to cloud adoption."[101] From a security perspective, one industry analyst opines that "[c]loud computing is optimized for performance, optimized for resource consumption, and optimized for scalability. It's not really optimized for security."[102] This analyst adds that "[a]t this early stage of the market, you have to be concerned with where security is now and whether vendors can bake it into their services from the start or try to bolt it on under pressure from customers."[103] At present, cloud computing is in many instances, still in its infancy.[104] As these initial cloud developers

[97] *Id.*

[98] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V 2.1, *supra* note 19, at 9.

[99] Some of the rare Level 4 and 5 certified organizations, such as Tata Consultancy Services, are service providers who use highly controlled service delivery processes. *See Corporate Facts*, TATA CONSULTANCY SERVICES, http://www.tcs.com/about/corp_facts/Pages/default.aspx (last visited Sept. 27, 2011). Nonetheless, one could argue that many private clouds that deploy any of the Service Models would likely have a maturity rating of between two and four, and public clouds would appear to be operating at maturity level of one or perhaps two. The rational for this assertion is that private cloud computing is similar in many ways to information technology outsourcing; a practice that has been utilized by businesses for a number of decades. *Cf.* SYMANTEC CORP., *supra* note 49, at 2.

[100] JONATHAN FELDMAN, INFORMATIONWEEK ANALYTICS, INFORMED CIO: CLOUD CONTRACTS AND SLAS 5 (2010), *available at* http://analytics.informationweek.com/abstract/5/2274/Cloud-Computing/informed-cio-cloud-contracts-and-slas.html.

[101] Tim Brown, *Cloud Security: Ten Questions to Ask Before You Jump In*, CIO (Jan. 26, 2010), http://www.cio.com/article/print/524214.

[102] Roiter, *supra* note 46.

[103] *Id.*

[104] The assertion that cloud computing is an immature technology is bolstered by statements along the lines of: "as technology such as virtualization and corresponding

implement cloud technology, the best advice is to "bring a parachute."[105] Thus, potential users of cloud services must look beyond just the apparent cost benefits and also consider the current maturity level and trajectory of their potential providers before surrendering their IT infrastructure control and critical data to such organizations. Further, some business sectors have special needs that must be considered, so the one-size-fits-all approach, frequently touted by public cloud services providers, requires particular scrutiny.

B. *The Five Foremost Distinguishable Business Sectors*

Businesses vary by size, sector, industry, and level of IT sophistication; each of which will require a different set of terms and goals to attain best practices and the most economical cloud usage. It is necessary to segregate businesses into various categories so as to provide a more directed application of the core principles, common terms, and specific negotiated terms that will be necessary for the ideal business maturity. Thus, a principles-based approach to privacy and security is necessary to adequately deal with the variety of issues that arise among various sectors. The five most distinguishable business sectors are small businesses, specialized businesses, medium-sized businesses, regulated large businesses, and the government sector.

1. Small and Medium-sized Businesses

In general, small businesses are independent businesses with a limited number of employees and a relatively low volume of sales.[106]

management services like automation, monitoring and capacity planning services become more mature, cloud computing will become more widely used for increasingly diverse and even mission-critical workloads." *See* IBM, *supra* note 54, at 5. A vendor suggests that one should "consider non-business critical applications that need to be scaled quickly as initial candidates for the cloud." *See* CAPGEMINI, *supra* note 41, at 12. Whereas an industry organization mentions "[c]loud computing is still a rapidly evolving landscape . . . ." *See* SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V 2.1, *supra* note 19, at 7.

[105] *See* FELDMEN, *supra* note 100, at 6. "All of this cloud computing attention creates an aura of excitement and hype. But like the electrically-charged clouds that collide in the sky, the hype emanating from cloud computing generates a lot of distracting flash and confusing noise." TYSON HARTMAN & LARRY BECK, AVANADE, DEFINING THE BUSINESS VALUE OF CLOUD COMPUTING 2 (2009), *available at* http://www.avanade.com/Documents/Research%20and%20 Insights/cloudpovfinalrevised090909874764.pdf. Because "not every use case is appropriate for cloud computing's [sic] current level of maturity," it seems that, in general, this environment might be most appropriate when used incrementally for use in pilots of non-critical business processes. *See* FELDMAN, *supra* note 100, at 6; *see also* ACCENTURE, *supra* note 12, at 3; SYMANTEC CORP., *supra* note 49, at 3; SHIPLEY, *supra* note 10, at 10.

[106] *See* U.S. SMALL BUS. ADMIN., TABLE OF SMALL BUSINESS SIZE STANDARDS MATCHED TO NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM CODES (2010), http://www.sba.gov/id

More specifically, however, the U.S. Small Business Association "defines a small business concern" as one that is:

> [O]rganized for profit; has a place of business in the U.S.; operates primarily within the U.S. or makes a significant contribution to the U.S. economy through payment of taxes or use of American product, material or labor; is independently owned and operated; and is not dominant in its field on a national basis. The business may be a sole proprietorship, partnership, corporation, or any other legal form.[107]

The Small Business Association has also established two primary and widely used size standards to define a small business: 500 employees (for most manufacturing and mining industries) and $7 million in average annual receipts (for most nonmanufacturing industries).[108] Examples of small businesses would include a small independent printing company, a local delicatessen meat market, and a local furnace or plumbing company.

While a small business refers to those with fewer than 500 employees, a medium-sized business refers to those businesses with more than 500 employees. Medium to large businesses are virtually self-explanatory in that they are all businesses that have not been deemed a small business by the U.S. Small Business Association.[109]

With respect to cloud services, both small and medium-sized businesses are particularly prone to privacy and security concerns. This susceptibility is primarily because small businesses lack the capital to build their own IT infrastructure. Additionally, because small businesses are competing in a larger market, they are often unable to attract, retain, and fund IT talent. This puts small businesses at a disadvantage in the cloud sector in terms of scrutinizing and negotiating with providers, but also makes the business case for migrating their services to the cloud very attractive, since such smaller organizations often struggle with marshalling the resources and allocating the time

c/groups/public/documents/sba_homepage/serv_sstd_tablepdf.pdf (enumerating small business size standards in millions of dollars and employees by industry).

[107] *What is a Small Business*, U.S. SMALL BUS. ADMIN., http://www.sbaonline.sba.gov/contractingopportunities/owners/basics/whatismallbusiness/index.html (last visited Sept. 27, 2011). The Small Business Association's statutory authority to determine whether a concern qualifies as a small business rests in the Small Business Act. 15 U.S.C. §§ 632(a)(1), 637(b)(6) (2006).

[108] *See* U.S. SMALL BUS. ADMIN., *supra* note 106. Small Business Size Regulations specifying size standards and governing their use are set forth in Code of Federal Regulations. 13 C.F.R. §§ 121.101-.1103 (2010).

[109] *See Businesses Determined Other Than Small*, U.S. SMALL BUS. ADMIN., http://www.sba.gov/content/businesses-determined-other-small (last visited Sept. 27, 2011).

required to deploy their own IT infrastructure. Thus, in order to continue to progress and develop their IT infrastructures along the maturity scale, small businesses need to deploy reliable cloud services rapidly to attain their goals and maintain a presence in the competitive market; this presents a challenge to the small business—as a category—with respect to sustainability in a world where cloud services are growing and prevailing.

2. Businesses Subject to Specific Regulations

Specialized businesses are those businesses that are subject to particular industry standards and regulations. Specific professions and industries, for example, are subject to various privacy and information protection regulations and industry standards, including: HIPAA,[110] SOX,[111] the Gramm-Leach-Bliley Act,[112] FTC Red Flags,[113] and FCC CPNI Rules.[114] The specialized businesses that are regulated by these and similar standards are often required to promulgate programs and strategies that address the security and privacy of personal and business-related information online.

Specialized businesses are the most regulated of the five sectors recognized in this Article. As such, it provides a normative framework specific to privacy developments and goals that can and should be applied to a broader spectrum of cloud computing agreements.

Regulated large businesses are similar to specialized businesses in that they are subject to professional and industry standards; however,

[110] *Understanding Health Information Privacy*, U.S. DEP'T OF HEALTH & HUM. SERV., http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (last visited Sept. 27, 2011).

[111] 15 U.S.C. §§ 7241-7246 (2006).

[112] *Id.* §§ 6801-6809.

[113] *Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy*, FED. TRADE COMM'N (Oct. 31, 2007), http://www.ftc.gov/opa/2007/10/redflag.shtm.

[114] *Protecting Your Telephone Calling Records*, FED. COMM. COMM'N, http://www.fcc.gov/guides/protecting-your-telephone-calling-records (last visited Sept. 27, 2011). Other regulations that may deserve mention could include the Electronic Communication Privacy Act (ECPA) because it has been interpreted to reduce one's fourth amendment rights when using cloud computing (vs. in-house computing), the USA PATRIOT ACT because it comes into play when the U.S. Government requests certain data that the user may not be able to provide based upon the laws governing the physical location of the server where the data in question is hosted, and the EU Data Privacy Directive because it dictates what data may flow from a country that has adopted these regulations (*i.e.*, Canada) to un-safe countries (*i.e.*, Iran and the United States). *See generally* Electronic Communication Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 (2006); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT), Pub. L. No. 107-56, 115 Stat. 272 (2001); European Parliament and of the Council Directive 1995/46 1995 Official J. (L281) 31 (EC).

they are different in that they operate on a much larger scale. An example of a regulated large business would be a major hospital network, which would be subject to HIPAA and state laws, among other regulations.

3. Government Sector

Last but not least is the government sector. Government agencies and public organizations around the world are moving their applications towards a "cloud approach."[115] However, in these cases, the "cloud" term calls for further scrutiny, because the deployment model selected, such as the targeted use of private and community clouds, is key. For example, in early 2010, U.S. Federal Chief Information Officer (CIO), Vivek Kundra, launched the government-sponsored and dedicated cloud computing services website, Apps.Gov, to showcase cloud and software options preapproved for use by federal agencies.[116] In a prepared statement, the Federal CIO said that "[o]ffering IaaS on Apps.gov makes sense for the federal government and for the American people."[117] He went on to state that "[c]loud computing services help to deliver on [the Obama] [A]dministration's commitment to provide better value for the American taxpayer by making government more efficient," in addition to driving innovation across all government sectors.[118]

To uniformly regulate the expansion of government action in the cloud, in October 2010, the White House launched the National Science and Technology Council—a new subcommittee focused on Privacy and Internet Policy.[119]

Recognizing the global nature of the digital economy and society, the Subcommittee will monitor and address global privacy policy challenges and develop approaches to meeting those challenges through coordinated U.S. Government action. The Subcommittee is committed

[115] *See* GILES HOGBEN, EUROPEAN NETWORK AND INFO. SEC. AGENCY, ENISA-CLOUD COMPUTING SECURITY STRATEGY 41, http://www.terena.org/activities/tf-csirt/meeting30/hogben-cloudcomputing.pdf (last visited Sept. 27, 2011). For example, Europe, Denmark, and the United Kingdom have become fast adopters, announcing the planning and implementation of cloud computing. *Id.*

[116] Rutrell Yasin, *11 Win GSA Cloud Computing Contracts*, WASH. TECH. (Oct. 20, 2010), http://washingtontechnology.com/articles/2010/10/20/apps-gov-adds-cloud-servcies.aspx.

[117] *Id.*

[118] *Id.*

[119] Cameron Kerry & Christopher Schroeder, *White House Council Launches Interagency Subcommittee on Privacy & Internet Policy*, THE WHITE HOUSE (Oct. 24, 2010, 10:10 AM), http://www.whitehouse.gov/blog/2010/10/24/white-house-council-launches-interagency-subcommittee-privacy-internet-policy.

to fostering dialogue and cooperation between our Nation and its key trading partners in support of flexible and robust privacy and innovation policies. Such policies are essential to the health of competitive marketplaces for online goods and services.[120]

The government sector is a large and complex sector, comprised of various entities, agencies, and interest groups. As such, it is faced with the challenge of striking the appropriate balance between the privacy expectations of consumers and the needs of industry, law enforcement and other public-safety governmental entities. Thus, government users are well-positioned to leverage their buying power and demand more mature practices from cloud service providers. Properly applied, such pressure can translate into more evolved services for all cloud services consumers, not just government users.

In another example, the U.S. Government has established the Federal Risk and Authorization Management Program, or FedRAMP, to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products.[121] FedRAMP provides joint authorization, which "results in a common security risk model that can be leveraged across the Federal Government."[122] FedRAMP also provides continuous security monitoring services for government and commercial cloud computing systems intended for multi-agency use.[123] This government-implemented common security risk model provides a consistent baseline for Cloud based technologies and ensures that the benefits of cloud-based technologies are effectively integrated across the various cloud computing solutions currently proposed within the government.[124]

Additionally, the NIST initiated the Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) program as a catalyst to help develop high-quality cloud computing standards.[125] The program attained this goal by providing "worked examples showing how key use cases can be supported on cloud systems that implement a set of documented and public cloud system specifications."[126] Based on these documented specific use cases, the SAJACC initiative plans to develop

[120] *Id.*

[121] *Federal Risk and Authorization Management Program*, CHIEF INFO. OFFICERS COUNCIL (Jan. 4, 2011), http://www.cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP.

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Standards Acceleration to Jumpstart Adoption of Cloud Computing*, NIST, http://www.nist.gov/itl/cloud/sajacc.cfm (last visited Sept. 27, 2011).

[126] *Id.*

tests and publish results on the SAJACC web portal.[127] The compilation of this data is intended "to provide pointers to known cloud system implementations, use case documents, upcoming events, and will also provide a convenient means to provide feedback to the SAJACC team."[128] The goal of this initiative is to reduce technical uncertainty and ensure high-quality security and privacy standards throughout the adoption and development of cloud computing.

C. *The Federal Trade Commission Provides Enduring "Core Principles" for Industry-Wide Regulation*

The FTC is an independent agency established by Congress in 1914 to enforce the FTC Act.[129] "Core principles" are those concepts and terms that any business—no matter the size and/or sector—should emulate when entering into a contract for cloud services to protect the privacy of the information stored.[130] The FTC has instituted a Privacy Initiative through the promulgation of a series of acts intended to create uniform and secure regulation of online content and to encourage active industry self-regulation.[131] This part suggests that the FTC Privacy Initiatives establish several very strong "core principles" that should be implemented into a business model to protect the privacy of personal and business-related information.[132] The FTC Privacy Initiatives offer businesses a comprehensive framework and practical starting point for incorporating core privacy principles into their business and computing model, while still taking advantage of the benefits of the cloud sector. Moreover, sector and market specific regulations offer further guidance but also impose constraints that must be considered when moving into the clouds.

1. Section 5 of the FTC Act: Enforcing Privacy Promises

Section 5 of the FTC Act prohibits unfair or deceptive practices.[133] This section of the Act is an integral element of the FTC's privacy initiative because it ensures that companies keep the privacy promises they make to consumers, including the precautions they take to secure

[127] *Id.*

[128] *Id.*

[129] *See* Act of Sept. 26, 1914, c. 311, § 1, 38 Stat. 717 (codified as amended at 15 U.S.C. §§ 41-58 (2006)).

[130] *See Privacy and Security*, BUREAU OF CONSUMER PROT. BUS. CTR., http://business.ftc.gov/privacy-and-security (last visited Sept. 27, 2011).

[131] *Id.*

[132] *Id.*

[133] 15 U.S.C. § 45 (2006).

consumers' personal information.[134] Section 5 of the FTC Act prohibits "unfair methods of competition" and was amended in 1938 to also prohibit "unfair or deceptive acts or practices."[135] In 1994, Congress amended section 5 of the FTC Act to provide that an act or practice is *unfair* if the injury it causes or is likely to cause to consumers is: (1) substantial; (2) not outweighed by countervailing benefits to consumers or to competition; and (3) not reasonably avoidable by consumers themselves.[136]

Section 5 was promulgated in response to consumers' concerns about privacy, and the result has been full disclosure. Many websites now post privacy policies that describe how a consumer's personal information is collected, shared, and secured;[137] "[a]lmost all the top 100 commercial sites now post privacy policies."[138] Demonstrating its commitment to ensuring privacy and protecting the public, the FTC has brought a number of cases to enforce the promises in businesses' privacy statements.[139] Section 5 of the FTC Act has effectively proscribed information practices that cause substantial injury to the consumer, and these apply to websites regardless of their deployment model.

2. The Gramm-Leach Bliley Act: Financial Privacy

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" (GLB Act), includes provisions to protect consumers' personal financial information held by financial institutions.[140] Compliance with the GLB Act is mandatory: there must be a policy in place to protect the information from foreseeable threats in security and data integrity whether a financial institution discloses non-public information.[141] There are three principal components to the

[134] *See id.* § 45(a)(2).

[135] Act of Mar. 21, 1938, c. 49, § 3, 52 Stat. 111 (codified as amended at 15 U.S.C. § 45(a)(1) (2006)).

[136] *See* 15 U.S.C. § 45(n)(1) (2006). The Commission previously relied on similar criteria to define the scope of its authority to prohibit unfair acts or practices pursuant to Section 5(a) of the FTC Act. *See, e.g., In re Orkin Exterminating Co.*, 108 F.T.C. 263, 362 (1986); *In re International Harvester Co.*, 104 F.T.C. 949, 1061 (1984); *see generally Federal Trade Commission Policy Statement on Unfairness*, 104 F.T.C. 949, 1070-76 (1984).

[137] *See Privacy and Security*, *supra* note 130.

[138] Steven T. Chinowsky, *Newly Enacted California Online Marketing Laws*, 1 CIPERATI 4 (2004), http://apps.americanbar.org/buslaw/committees/CL320010pub/newsletter/0004/.

[139] *See Making Sure Compaines Keep their Privacy Promises to Consumers*, FED. TRADE COMM'N, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last modified Sept. 6, 2011).

[140] *See generally* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-6809 (2006).

[141] *Id.* § 6801(a).

privacy requirements: (1) the Financial Privacy Rule;[142] (2) the Safeguard Rule;[143] and (3) the Pretexting Provision.[144]

The Financial Privacy Rule requires that financial institutions give their customers privacy notices.[145] These notices must explain the collection and sharing practices of the financial institution.[146] This gives customers the right to limit some sharing of their information, and even opt out of the information being shared with unaffiliated parties.[147] Also, financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information.[148]

The Safeguards Rule requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information.[149] The Safeguards Rule is broad in that it applies to the information of any consumers, past or present, of the financial institution's products or services.[150] This privacy and security plan must (1) assign at least one employee to manage the safeguards; (2) construct a thorough risk management to identify internal risks; (3) develop a monitoring and testing program to secure the information; and (4) provide adaptable safeguards as needed that will remain compatible with the changes in how information is collected, stored, and used.[151] This rule has proved to be practical and business-savvy; it forces financial institutions to take a closer look at how they manage private data and to conduct risk analysis on their current processes. These proactive steps allow a business to critically analyze its current process, which will inherently help the business to attain its optimal maturity level.

The pretexting provision of the GLB Act protects consumers from

[142] *Id.* For a summary overview of the Financial Privacy Rule, see *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, BUREAU OF CONSUMER PROT. BUS. CTR. (2002), *available at* http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act.

[143] 15 U.S.C. § 6801(b).

[144] *Id.* § 6821(a).

[145] *See id.* §§ 6802-6803.

[146] *Id.* § 6803(a). On November 17, 2009, eight federal regulatory agencies released the final version of a model privacy notice form to make it easier for consumers to understand how financial institutions collect and share information about consumers. *See Federal Regulators Issue Final Model Privacy Notice Form*, SEC. & EXCH. COMM'N (Nov. 17, 2009), http://www.sec.gov/news/press/2009/2009-248.htm.

[147] 15 U.S.C. § 6802(b)(1) (2006).

[148] *Id.* § 6802(d)-(e).

[149] *Id.* § 6801(b)(1).

[150] *Id.* § 6803(a)(1)-(2).

[151] Thomas J. Smedinghoff, *Complying with the GLBA Safeguards Rule: What Financial Institutions Must Do to Avoid Data Breach*, KNOL (July 29, 2008), http://knol.google.com/k/rob-scott/complying-with-the-glba-safeguards-rule/1llgytainraw9/1#.

individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting."[152] Pretexting is also often referred to as social engineering, which occurs when someone tries to gain access to personal, non-public information without the authority to do so.[153] The GLB encourages financial institutions to implement safeguards against pretexting.[154] A privacy plan intended to satisfy GLB's Safeguards Rule—to protect consumers from third parties obtaining their personal information under false pretenses—would require an employee training initiative to educate employees on potentially fraudulent activity.[155] Combined, these three rules provide a comprehensive plan to insure privacy and security protection for personal financial information and again, apply regardless of deployment model.

3. Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) promotes accuracy in consumer reports and is meant to ensure the privacy of the information contained within.[156] The FCRA was recently amended by the Fair and Accurate Credit Transaction Act (FACTA) of 2003.[157] The FACTA requires the Commission and other agencies to implement many of the new provisions of the FCRA by means of rules and regulations.[158] These Acts form the base of consumer credit rights in the United States, and those organizations that impact consumer credit reports must consider the implications, whether they retain control of their IT infrastructure or migrate to the cloud.[159]

4. Children's Online Privacy Protection Act

The primary goal of the Children's Online Privacy Protection Act

[152] 15 U.S.C. §§ 6821-6827 (2006).

[153] *Gramm-Leach-Bliley ACT Check*, EC-COUNCIL GLOBAL SERVS., http://www.eccouncil.org/egs/GLBACheck/GLBACheck.html (last visited Sept. 27, 2011). This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "phishing" (*i.e.*, using a phony website or email to collect data). *Id.*

[154] 15 U.S.C. § 6801(b).

[155] *The Gram-Leach Bliley Act (GLBA) Fact Sheet*, Wiresoft (Feb. 14, 2009), www.wiresoft.net/_literature_43482/GBLA_Fact_Sheet.

[156] 15 U.S.C. § 1681.

[157] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

[158] *See* 15 U.S.C. § 1681s (2006).

[159] *See id.* § 1681a. In addition to credit reports on file with credit bureaus and consumer reporting agencies, the FCRA may govern other files of information collected and maintained on consumers, depending on their content and use. Medical information, and information used to prevent and detect fraud, are sometimes governed by the FCRA. *See id.*

(COPPA) is to give parents control over what information is collected from their children online and how such information may be used.[160] COPPA is very broad, both in terms of who is subject to the rule and the scope of the rule. The rule applies to:

> operators of commercial websites and online services directed to children under 13 that collect personal information from them; operators of general audience sites that knowingly collect personal information from children under 13; and operators of general audience sites that have a separate children's area and that collect personal information from children under 13.[161]

COPPA provides a broad scope of guidance: it requires the operator to post a privacy policy on the homepage of the website, when to seek verifiable consent from a parent or guardian, when and how to offer parents an opportunity to delete a child's personal information, and other practices an operator must pursue to protect children's privacy and safety online, including restrictions on marketing to those under 13.[162] Additionally, to encourage active industry self-regulation, COPPA includes a safe harbor provision, which allows industry groups and others to request FTC approval of self-regulatory guidelines to govern participating websites' compliance with the rule.[163] Thus, cloud services that support websites directed to children must provide COPPA-compliant support.

[160] Children's Online Privacy Protection Act of 2003, 15 U.S.C. §§ 6501-6505 (2006); *Frequently Asked Questions About the Children's Online Privacy Protection Rule*, FED. TRADE COMM'N, http://www.ftc.gov/privacy/coppafaqs.shtm (last updated Oct. 7, 2008).

[161] *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, FED. TRADE COMM'N, http://www.ftc.gov/privacy/coppafaqs.shtm (last updated Oct. 7, 2008).

[162] *See* 15 U.S.C. § 6502(b); *Compliance Reports: COPPA Requirements*, AppsCan Enterprise Edition/Policy Tester, RATIONAL SOFTWARE; http://publib.boulder.ibm.com/infocenter/asehelp/v5r5m0/index.jsp?topic=%2Fcom.ibm.ase.help.doc%2Ftopics%2Fr_coppa_report.html. The Rule requires operators to: post a privacy policy on the homepage of the website and link to the privacy policy on every page where personal information is collected; provide notice about the site's information collection practices to parents and obtain verifiable parental consent before collecting personal information from children; give parents a choice as to whether their child's personal information will be disclosed to third parties; provide parents access to their child's personal information and the opportunity to delete the child's personal information and opt-out of future collection or use of the information; not condition a child's participation in a game, contest or other activity on the child's disclosing more personal information than is reasonably necessary to participate in that activity; and maintain the confidentiality, security and integrity of personal information collected from children. FED. TRADE COMM'N BUREAU OF CONSUMER PROT., YOU, YOUR PRIVACY POLICY AND COPPA-HOW TO COMPLY WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT 1 (2002), http://business.ftc.gov/documents/bus51-you-your-privacy-policy-and-coppa-how-comply-childrens-online-privacy-protection-act.pdf.

[163] 15 U.S.C. § 6503(a) (2006).

VI. SHELTER FROM THE STORM

Consumer demand has facilitated the rapid adoption of cloud computing services. Further, a demand for reasonable risk management approaches and support for regulatory compliance by those same consumers may influence even the largest providers in today's competitive environments, especially if large enterprise and government customers leverage their buying power. Potential adopters of cloud services should assess their information assets and potential risks to insure that these protective controls are included as a part of the service level agreement (SLA) negotiated with the provider.[164] Bargaining power often favors the cloud services provider in today's environment; regulatory intervention requiring basic adherence to fair information practices and disclosure of risks will provide welcome shelter for cloud services consumers.[165]

The informed consumer and those with a healthy sense of paranoia regarding their risks do have resources available, especially in the areas of risk identification and security. The Cloud Security Alliance maintains a thorough and increasingly influential set of guidance that includes privacy and security risks.[166] Regulators are also taking notice of cloud computing issues, although perhaps still in a fact-finding mode, as noted in the Federal Trade Commission Chairman's 2010 Annual Report.[167] Finally, through its Global IT Council for Cloud Services, Gartner has published seven rights and responsibilities of cloud services consumers as a call to service providers for action and a checklist for consumers to reference:

1. The right to retain ownership, use and control of one's own data;

2. The right to service-level agreements that address liabilities, remediation and business outcomes;

3. The right to notification and choice about changes that affect the

[164] "[T]he SLA is one of the most effective tools the enterprise can use to ensure adequate protection of information entrusted to the cloud." INFO. SYS. AUDIT AND CONTROL ASS'N, CLOUD COMPUTING: BUSINESS BENEFITS WITH SECURITY, GOVERNANCE AND ASSURANCE PERSPECTIVES 8 (2009).

[165] Some commentators have cautioned consumers regarding the ability of regulators to intervene at this time, stating, for example, "[d]on't bother looking to state or federal government entities or industry groups for help just yet. They're simply not moving fast enough to keep up with the pace of technology." Fratto, *supra* note 59, at 36.

[166] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V 2.1, *supra* note 19, at 7.

[167] THE FTC IN 2010: FEDERAL TRADE COMMISSION ANNUAL REPORT, *supra* note 68, at 40.

service consumer's business processes;

4. The right to understand the technical limitations or requirements of the service up front;

5. The right to understand the legal requirements of jurisdictions in which the provider operates;

6. The right to know what security processes the provider follows;

7. The responsibility to understand and adhere to software license requirements.[168]

Ultimately, only the business "consumer"—whether a small business, individual, or large enterprise—can decide whether the business benefits of cloud computing services outweigh the risks. A thorough understanding and classification of one's information assets is critical to making an informed decision, particularly in today's environment of lagging regulation and powerful service providers. Particular concerns, including the ability to meet regulatory obligations, must be addressed more carefully for those individuals and organizations that create, access, transmit, or otherwise manage highly sensitive personal information.

The "core principles" should be emulated by industries and organizations nationally and internationally to ensure strategic, safe, and secure cloud computing opportunities. FTC Privacy Initiatives establish several very strong "core principles" that should be implemented into business models of all sizes to protect the privacy and security of personal and business-related information. The FTC Privacy Initiatives offer businesses a comprehensive framework and a practical starting point for incorporating core privacy principles into their business model, while still taking advantage of the benefits of the cloud sector.

CONCLUSION: A CALL TO ACTION

Andy Grove, long time Intel CEO, once stated that we, as citizens in society, cannot stop technological development.[169] In the face of such ever-accelerating innovations, the treatment of privacy, security, and

[168] GARTNER, INC., GARTNER GLOBAL IT COUNCIL FOR CLOUD SERVICES 1 (2010), *available at* http://www.gartner.com/technology/research/reports/global-it-council.jsp.

[169] *See, e.g.*, Mr. Grove's commentary on how "Only the Paranoid Survive" in light of technological developments and Strategic Inflection Points," at http://www.intel.com/pressroom/archive/speeches/ag080998.htm (last visited Sept. 30, 2011).

other core risk issues has had its ups and downs as technology has advanced. Society must help avert the coming storm in cloud computing by gently guiding technology to achieve efficiency and financial benefits, while reasonable privacy, security, and other risk management interests are protected. As the five major business sectors embrace cloud technology, they will each evolve through the Carnegie Mellon Software Engineering Institutes Capability Maturity Integration (CMMI) Model at a different pace, and with different considerations in mind. To establish a normative framework, the FTC core privacy principles must be incorporated at each step and in all agreements, as each business sector progresses through the CMMI Model. By faithfully incorporating these FTC core privacy principles into service provider agreements, privacy rights can be sheltered from the storm.