Silicon Flatirons

A Center for Law, Technology, and Entrepreneurship at the University of Colorado

*Roundtable Series on Entrepreneurship, Innovation, and Public Policy**

Cybersecurity and Cloud Computing in the Health Care and Energy Sectors:

Perception and Reality of Risk Management

Matt Burns, Rapporteur†

June 2013

Colorado Law
University of Colorado Boulder

*The Silicon Flatirons Roundtable Series on Entrepreneurship, Innovation, and Public Policy is sponsored by Brad Feld, Managing Director of the Foundry Group. This is the 31st Flatirons Report. More Reports – on topics including private equity, internet governance, cloud computing, angel investing, and modern pedagogy – can be found at http://www.siliconflatirons.com/publications.php?id=report. Roundtable and Summit discussions further the Silicon Flatiron Center's goal of elevating the debate around technology policy issues

† Research Fellow, Silicon Flatirons Center. Thanks also to Laura McNabb, Melodi Gates, and Ben Abell for their valuable comments and edits

Executive Summary

Cloud computing promises to enable new frontiers of innovation and convenience. As a result of this emerging technology, services that would have required significant capital expenditures just a few years ago are now available in a pay-per-use model, if they cost end users anything at all. Increasingly, cloud services enable everyday technologies, and often the end user is not aware that cloud computing is involved. Innovation, convenience, and speed are the baseline expectations for the growing number of digitally connected people in the world.

The health care and energy sectors are not immune from the pressure to fully integrate into the connected world. However, these sectors are highly regulated by government entities, are mission critical systems (that is, people depend on them), and handle some of their customers' most private and sensitive information. For these reasons, many health care and energy organizations have resisted the move to cloud computing on a standardized enterprise level. Today, these organizations face the ramifications of their own employees' and customers' unregulated use of these technologies, inadvertently creating an enterprise risk they are now forced to confront. The critical questions for organizations in these sectors are: what are the real risks of different types of cloud computing, and in light of these risks, how can organizations in these sectors make better choices with respect to the cloud?

To address these questions, the Silicon Flatirons Center convened 43 leaders from the legal, academic, and business community (collectively, "the Roundtable") on January 10, 2013. The Roundtable discussed the risks of cloud computing and how businesses generally, and the health care and energy sectors specifically, can manage these risks. The main objectives of the Roundtable included identifying legal and regulatory risks involved in adopting cloud technology, identifying potential pitfalls, and identifying management and governance solutions that can increase data security and privacy while improving organizations' end products.

The Roundtable featured a range of perspectives on these questions. The discussion included a variety of ideas and opinions, some of which did not garner consensus among the group. Other perspectives gained wider support. In particular, three key themes emerged from the January 10th Roundtable discussion.

There is a difference between the perception of the risks of cloud computing and the reality of those risks. As with many new technologies, incomplete information and early incidents can shape a persistent perception that in the long run proves false. Cloud computing is no different. What is important to understand about cloud computing as compared to many technologies that have come before it is that cloud computing processes user data on third-party servers in the background of consumer-facing applications. These applications are being rapidly adopted by individuals and service providers, often resulting in an organization's data residing on cloud service provider hardware without the organization's knowledge or intention. Given this rapid adoption of cloud-based services, even organizations that actively work to avoid them may find it impossible to avoid them entirely. In light of this dynamic, understanding and managing the risks of cloud computing, and

applying that understanding to an enterprise risk management strategy, is critical for nearly all organizations.

Organizations in the health care and energy sectors can responsibly and beneficially utilize cloud computing. Despite the regulatory burdens and highly sensitive information that organizations in these sectors must manage, there are still opportunities to adopt cloud technologies in ways that can be beneficial to these organizations and to their consumers while maintaining—or even increasing—data security and privacy. It is critical for these organizations to carefully consider each aspect of their business as it relates to information technology needs and risks, and then determine where cloud services are appropriate (or inappropriate) for serving those needs. These risk management principles apply with equal force whether or not the organizations' activities occur on the cloud.[1] Therefore, a careful examination of both the information technology risk management principles and the risks of conventional and cloud computing is necessary for optimum risk management.[2]

Regulating the cloud is a challenging undertaking that must be addressed with great care. Cloud computing has rapidly become an important technology that is used in many people's daily lives. The speed at which cloud computing has been adopted has far outpaced the ability of regulators and lawmakers to develop effective regulations. However, this lack of regulation has an upside, as regulating the cloud, or regulating a particular sector's use of the cloud, is very difficult to get right. A poorly crafted regulatory structure might not only fail to prevent the harms it is intended to prevent, but may also chill innovation, robbing organizations of efficiencies and customers of services. Rather than regulating cloud computing or its use, regulations are more likely to be successful if they address the security and privacy expectations of organizations, compelling those organizations to find innovative solutions to meet those expectations.

[1] Charles M. Horn & Chris Ford, *Security, Privacy Issues Engage Financial Firms Looking Into Cloud Computing*, 100 BBR 71, 4 (January 8, 2013).
[2] *Id.*

Table of Contents

Introduction

There is a gap between how individuals and organizations perceive the risks of cloud computing and the reality of those risks. Like other activities, the actual risk of cloud computing may be inconsistent with common perceptions.[3] This Report will help close the gap between perception and reality to help decision-makers, both in companies and government, make better choices regarding cloud computing.

This Report proceeds in four parts. Part I presents the key attributes of cloud computing necessary for understanding the risks of the cloud. Part II identifies key risk profiles in cloud and conventional computing. Part III shifts the focus to the health care and energy sectors, addressing specific risks and benefits of cloud computing in these sectors. Finally, Part IV briefly addresses the challenges of regulating the cloud and provides recommendations.

I. Cloud Basics: What is a Cloud?

It is necessary to first define what "cloud computing" is, and also what it is not. As Colorado Law Professor Paul Ohm noted, most people perceive "the cloud" as a monolith. The reality is that clouds, as the name implies, are amorphous and constantly changing. They come in many different flavors. For the purposes of this Report, a cloud can be thought of as a set of remotely accessible computing resources that can be dynamically reconfigured based on user demand.[4] These resources are typically used on a contract basis in lieu of user-owned computing resources.[5] Google, for example, offers several cloud-based services; Gmail and Google Drive[6] (formerly Google Documents) are free and familiar to many, but there are also fee-based services like Google Compute Engine[7] and Google Cloud Storage.[8] For the purposes of this Report, "the cloud" refers to one or more of these kinds of resources.

These resources tend to break down into three categories: (1) software as a service ("SaaS"), where the software applications are hosted by a cloud service provider ("CSP") and accessed remotely by users; (2) platform as a service ("PaaS"), where development tools are hosted by a CSP and accessed remotely; and (3) infrastructure as a service ("IaaS"), where the user is outsourcing the physical hardware (e.g., servers) needed to support its operations, but the system remains dedicated to that user.[9] The key aspect of all three types of cloud

---

[3] The archetypal example is driving versus flying. Flying can be shown to be significantly more safe than driving, but most people will admit to perceiving it to be more risky. *See* Michael Sivak & Michael Flannagan, *Flying and Driving after the September 11 Attacks*, AMERICAN SCIENTIST, http://www.americanscientist.org/issues/issue.aspx?id=3312&y=0&no=&content=true&page=2&css=print (last visited May 1, 2013).

[4] Luis M. Vaquero, et al., *A Break in the Clouds: Towards a Cloud Definition*, 39 COMPUTER COMM. REV. 50, 51 (2009).

[5] *Id.*

[6] The two services are now connected for large file transfer. Thomas Claburn, *Google Links Gmail to Drive for Huge Attachments*, INFORMATIONWEEK, http://www.informationweek.com/cloud-computing/software/google-links-gmail-to-drive-for-huge-att/240142664 (last visited May 1, 2013).

[7] *See* GOOGLE COMPUTE ENGINE, https://cloud.google.com/products/compute-engine

[8] *See* GOOGLE CLOUD STORAGE, https://cloud.google.com/products/cloud-storage

[9] TIMOTHY GRANCE & PETER MELL, NAT'L INST. OF STANDARDS AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (Hereafter "NIST Definition").

service is that the user's data is being handled, processed and stored, temporarily or otherwise, by the CSP on the CSP's systems.

Each of these services can be hosted on one (or more) types of cloud infrastructure. The United States' National Institute of Standards and Technology ("NIST") has identified four models: the "private cloud," the "public cloud," the "community cloud," and the "hybrid cloud."[10] A private cloud is a system that operates with the resource flexibility of a cloud, but serves only one organization.[11] The community cloud model is essentially a semi-private cloud that is shared by several related organizations.[12] The public cloud is the one that most of us are likely familiar with (as a result, there is often a perception that data on a cloud is on a public cloud and exposed to the risks of a public cloud, which is often not the case). In a public cloud, the CSP makes computing resources (including storage) available to the general public for a fee that is typically tied to actual usage.[13] A hybrid cloud is one where resources from more than one type of cloud service are used.[14] While many of the risks of cloud computing are similar across all cloud types, the specific risk profiles of these services can vary.

II. What are the Real Risks of Cloud Computing as Compared to Conventional Computing?

It is important to identify the differences between cloud computing and conventional computing from a risk assessment and management standpoint. The perception is that the cloud is a higher-risk environment with respect to data privacy and security than conventional computing. The reality is much more nuanced.

The common perception of cloud computing is that it presents a risk to privacy and data security. This is true, but an incomplete analysis. The correct analysis, based on the reality of cloud computing, should aim to determine in what ways the risk profiles of the various types of cloud computing differ from the risk profiles of conventional computing and, with these risk profiles in mind, whether the benefits of cloud computing as compared to conventional computing are significant enough to make cloud computing the correct choice for some or all of an organization's computing needs. This analysis is different for each organization based on that organization's information technology resources and needs; what is presented herein is a framework rather than a one-size-fits-all analysis tool. This section will work through elements of this analysis beginning with a look at the realities of the modern computing environment. This section will then address the net risks and benefits of cloud computing and will conclude with suggestions for an organizational approach to decision-making with respect to computing choices.

a. Your Company is Probably Using the Cloud Whether You Like It or Not

[10] *Id* at 3.
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*

As Patrick Heim, Chief Trust Officer of Salesforce.com, pointed out, most companies are already using the cloud whether or not they know about or intended such use. The perception is that the use of cloud computing is a yes/no choice that an organization's executives or IT departments can make; if they want to prevent their data from ending up on the cloud, they simply don't purchase cloud-based software. The reality is that for many companies, it is too late because they are already using cloud-based services through their employees' activities.

Heim pointed out the issue of the "cloud native" population. These are people who are accustomed to using the cloud and will continue to do so, even if their employers instruct them not to. He noted that while the cloud can empower the individual, it can also allow for the bad choices of individuals to harm organizations. The cloud is broadly present and enables software that is often very robust, simple to use, and cheap. These traits make it very easy for individuals and organizations to interact with the cloud.

An organization's data can end up on a CSP's systems through "planned use" and "unplanned use." Unplanned use is when an organization's data ends up on cloud resources without the express intention of the organization to use cloud resources for that data (think employees using a service like Google Drive or Dropbox to move files between their office and home computers without permission from the organization). Planned use is when an organization, by policy or contract, uses a CSP to provide computing or storage services.

Unplanned use of the cloud can occur through use of mobile device applications and web-based services like Gmail and Google Drive. The low cost of many cloud resources means that "the normal processes and procedures an organization uses to acquire computational resources as capital expenditures may be easily bypassed by a department or an individual[] and… obscured under day-to-day operational expenses."[15] Stated another way, where software, storage, or computer capacity in conventional computing used to be a decision that required multiple approvals, cloud services (which cost little or nothing) bypass this formal review system and often go undetected by managers. This is a significant concern among IT professionals in American and European organizations.[16]

In addition to unplanned cloud use by company personnel, a company's data can find its way onto the cloud through subcontractors and sub-subcontractors. As Danny Weitzner, MIT professor and former Deputy Chief Technology Officer at the White House explained, it would be incorrect to assume that organizations are not on the cloud already because many organizations are dependent on subcontractors who are dependent on the cloud. While service agreements between the prime contractor and subcontractors may contain specific security provisions, it becomes more and more difficult to ensure security down the chain.[17] Further, it is unreasonable to assume that subcontractors don't have the same unplanned cloud use problems that the prime contractor has.

---

[15] WAYNE JANSEN & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF STATE, SPECIAL PUB. NO. 800-144, GUIDELINES ON SECURITY AND PRIVACY IN CLOUD COMPUTING 14 (2011). (Hereafter "NIST Guidelines")

[16] *Id* at 15.

[17] *See* Siani Pearson & Azzedine Benameur, *Privacy, Security and Trust Issues Arising from Cloud Computing*, 2010 IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE 693, 698.

i. Your Consumers Will Demand Services that the Cloud Can Enable

The "cloud native" population that Patrick Heim noted above is not isolated to IT professionals or company employees. It is becoming a larger and larger part of the consumer base of many companies. He notes that consumers expect everything online. This expectation goes beyond low-security or entertainment uses like listening to music through Apple's iCloud or Netflix's streaming service. Justin Segall, co-founder of Simple Energy, noted that energy customers are being engaged and empowered through the use of data. Melodi Gates, a lawyer at Patton Boggs, pointed out that patients want access to records and won't be tolerant of delays. Similarly, as eBay's Scott Shipman noted, unlike in the energy industry, consumers in the health care industry have a choice and can make their demand for the convenience of cloud-based services felt by leaving providers that do not offer them.

b. The Net Risks of Cloud Computing

As noted above, the perception is that using the cloud creates a larger risk to data than using conventional computing. The reality is that from the first IBM technician to spill coffee on a stack of punch cards to highly sophisticated modern malware, data has always been at risk and cloud computing simply presents a different risk profile. In some cases conventional computing can be more high-risk than cloud computing. Of course, risk must also be viewed in relation to the potential benefit of the activity that creates the risk, so organizations must weigh the value of adopting cloud computing against the risks. This section will address the gap between the commonly perceived risks of cloud computing and real risks that are specific to or exacerbated by cloud computing.

i. Cloud-Specific Risk Profiles

There are a few risks commonly identified with cloud computing that result from the nature of the technology. CSPs are (generally) independent businesses with physically remote facilities.[18] They take advantage of flexible and dynamic assignment of resources to users as demand changes.[19] They also take advantage of economies of scale by centralizing services. Each of these traits creates a risk profile that is different from conventional computing.

Unlike conventional computing, where the data remains on the in-house servers,[20] using cloud services means that data exists on the CSP's systems, which are not under the data owner's control. The dynamic nature of cloud computing can make it difficult to track the particular CSP systems, and even the country, in which the data resides.[21] Cloud computing, as a result, can make it difficult to be certain of compliance with regulations or contractual obligations that demand that data remain within (or outside of) a particular location or country.[22]

---

[18] *See* NIST Guidelines, *supra* note 15, at 12, Pearson, *supra* note 17, at 693.
[19] *See* NIST Definition, *supra* note 9, at 2.
[20] Except when it doesn't: see section II.a. above regarding unplanned cloud usage.
[21] Pearson, *supra* note 17, at 693.
[22] Risks of cross-border data flow include host country laws that allow access by that country's law enforcement agencies, as permitted in the United States by the USA PATRIOT Act and European laws that prohibit storage of data in countries with weak data privacy laws. *Id.* at 698.

Another issue that arises from this remote location of a user's data is the potential for the CSP to cease operations. If a CSP becomes bankrupt or is acquired by another company, what happens to the data?[23] As Gates noted, having a mechanism to know where data is and having the ability to retrieve it at any time is a critical issue. These data location and retrieval issues make thorough due diligence with respect to the business stability of the CSP and capacity for data retrieval critical for organizations considering cloud computing.

The flexible nature of cloud systems creates a few situations unique to shared platforms. First, there are no physical barriers between "computers" when multiple clients are running virtual machines or sharing storage space, which creates different opportunities for attacks.[24] Second, the way data is moved and processed, which is part of what makes cloud computing so effective, also creates new avenues of attack.[25] Third, typically when a user completes a computing process, the data is not deleted from the physical hardware.[26] Instead, the computer is told that the space is now available for use, but the remnant data remains until it is overwritten.[27] It is possible to read deleted data from this hardware if it is not wiped or overwritten.[28] Complicating matters is the fact that many CSPs store data redundantly in many different locations, information that is unavailable or not disclosed to the user.[29] As such, it is difficult to ensure that a CSP has wiped or overwritten data.

Finally, the sheer volume of data that is held by many CSPs creates a tempting target. Where an individual computer or server system may hold a company's most sensitive information, a CSP's systems may hold sensitive information from dozens of companies. As Ashkan Soltani, an independent researcher and consultant, noted, if an attacker can get into one CSP, he or she can access a very large number of data sets. The analogy is robbing a bank instead of robbing a large number of individuals: the cloud has a scale problem that conventional computing rarely has. This makes CSPs a popular target for attacks and as Weitzner pointed out, when things go wrong with cloud computing, they go very wrong for a lot of people.

ii. Security and Reliability Benefits of Cloud

While the above descriptions of the risks of cloud computing, combined with anecdotes like the recent Netflix/Amazon service interruption,[30] tend to drive the perception that cloud computing is less secure and reliable, it is important to recognize that in reality a diligent CSP can do a much better job of securing data than a particular individual or company can in many cases (even with data that is not on the cloud).

---

[23] *Id.* at 694

[24] NIST Guidelines, *supra* note 15, at 11.

[25] *Id* at 28.

[26] Pearson, *supra* note 17, at 695. Note that this is generally true for conventional computing as well, but in conventional computing, the hardware is not made available for other users.

[27] NIST Guidelines, *supra* note 15, at 31.

[28] *Id.*

[29] *Id* at 17.

[30] On Christmas Eve 2012, Amazon Web Services, which hosts Netflix, experienced an interruption that took Netflix (among other services) down for several hours. *See* Julie Bort, *Amazon Explains Why It Took Netflix Offline On Christmas Eve*, BUSINESS INSIDER (Dec. 31, 2012), http://www.businessinsider.com/amazon-apologizes-for-netflix-outage-2012-12.

Patrick Heim listed several additional reasons why, despite the additional risks noted above, CSPs can do a better job securing data than can many companies using conventional computing. First, the risk environment to data is constantly changing and the response times can be faster in a cloud environment. Second, with cloud computing, there is an element of common defense. Good security requires highly skilled professionals; such professionals are hard to come by and expensive. A small company's catch-all IT professional is unlikely to have this level of skill, meaning that many companies don't have anyone with sufficient cybersecurity expertise. Reputable CSPs do have the capacity to hire security experts. In essence, the question becomes whether you want to hide your data in the wilderness and hope to be ignored, or place your data inside of a defended fortress that is more likely to be the target of attack. To continue the bank analogy from above, it would be like deciding between keeping your money in a simple safe at home and securing it in a sophisticated bank vault.

c. Approaches to Cloud Computing and Security

The perception of cloud computing as a risky and unknown system pushes many organizations to take an avoidance or compliance approach. These organizations attempt to avoid the cloud entirely, or, if they do use it, rely on compliance with a checklist to ensure security. The reality of the complex, nuanced, and constantly changing risk profile of cloud computing demands instead an active, opportunistic, entrepreneurial strategy that aims to understand and manage risk in a way that creates competitive advantages.

The avoidance/compliance mindset is a passive approach. Organizations accepting the perceived risks of the cloud as reality may choose to do nothing, thinking they can avoid the problem by avoiding the cloud. As we have noted above, avoiding the cloud is nearly impossible. Those organizations that approach the cloud defensively through compliance audits are also at risk. Dirk Anderson, Managing Director of Coalfire, called this the "binder exercise" in which an organization pulls out the compliance binder once a year, runs through a checklist to ensure it is "secure" and then forgets about security for another year. Unfortunately, by the time the rules for an audit are written down and placed in the binder, they are likely obsolete. For these reasons, compliance audits may be a necessary piece of a security system, but are not alone sufficient.

A better approach, supported by several participants at the roundtable, was the active risk management approach: an ongoing process of continual risk assessment, exploration of mitigation strategies, and application of those strategies to prevent harm. Organizations taking this active risk management approach recognize that compliance does not equal security. Rather than attempting to avoid using the cloud, these organizations recognize where using the cloud can add value and where it adds substantial risk. Understanding and managing this risk is a substantial undertaking, and organizations must dedicate appropriate thought to this process.[31] They educate employees. They examine the data they collect, handle, and produce and decide on appropriate risk profiles for the data sets. They put data on the cloud when appropriate (and on the appropriate type of cloud), and keep particularly

[31] Doug DePeppe of i2 IS Corporation noted after the Roundtable discussion that this is a substantial, and potentially unmanageable undertaking for much of our society. Without a doubt, understanding and managing risk in the cloud requires significant knowledge and energy.

sensitive data off of the cloud.[32] They are innovative with their use of the cloud in ways that add value. As Scott Shipman pointed out, most companies' core competencies are not in IT management. Judicious use of CSPs for appropriate IT functions can give companies more bandwidth to focus on their core business.

An active risk management approach can also allow companies to focus on reducing the risks to data that they are uniquely able to address: the risk of a privacy or security breach resulting from actions of personnel within their organization. Untrained, careless, or rogue employees can create a damaging data breach for a reputable CSP. Chris Roberts of One World Labs noted that his group of security testers was able to gain access to a system using something as simple as a bottle of vodka. Techniques like this are often called social engineering and are particularly attractive because employees are vulnerable entry points for cyber attacks.[33] Employees must be aware that they must act as a line of defense; training them to prevent this kind of insider risk is critical.[34] Even loyal and dedicated employees who are careless with passwords or a thumb drive can cause significant data leakage.

III. How Can the Health Care and Energy Sectors Responsibly Utilize Cloud Computing?

The perception of the cloud as a high-risk environment for organizations with sensitive data would seem to dictate that any such organization should avoid cloud computing entirely. The reality is that the health care and energy sectors can use cloud computing to make the valuable innovations that consumers (and increasingly, regulators) demand. This section will address specific steps organizations in the health care and energy sectors can take to maximize utility, remain competitive, and keep their data secure.

a. General Themes

The first step for both health care and energy sector organizations is to identify what data should and should not be on the cloud (and if a public or private cloud is more appropriate). Specific types of data that carry personally identifiable information ("PII") or other restricted information that can result in heavy sanctions[35] if leaked may not be appropriate for the cloud. However, in health care and energy organizations, like virtually any other organization, not all data is sensitive. Large amounts of data may be innocuous,[36] and other sets of data may fall into a risk profile that would make a private cloud appropriate. The key for these organizations is to think carefully about the sensitivity level of different kinds of data and handle it appropriately.

---

[32] Ashkan Soltani noted, however, that if someone has enough data that is itself not sensitive data but relates to sensitive data, that person may be able to infer the substance of the sensitive data.

[33] Patricia Titus, *I am the difference between "at risk" and "at ease"*, SYMANTEC (Nov. 1, 2012), http://www.symantec.com/connect/blogs/i-am-difference-between-risk-and-ease.

[34] *Id.*

[35] Depending on the level of culpability of the institution in the incident, penalties under the HITECH Act's modifications to HIPAA can vary from $100 to $50,000 *per violation* (each separate patient file whose privacy is breached is a single violation), with maximum penalties topping out at $1,500,000. HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123 (Oct. 30, 2009) (to be codified at 45 C.F.R. pt. 160), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf. Additionally, as Erika Bol pointed out, federal regulators have expanded the definition of "business associate" to include any contractor that maintains protected health information on behalf of a covered entity, thus potentially expanding liability to cloud providers.

[36] However, as Soltani noted, if one has enough access to non-sensitive data, one can make inferences about sensitive data.

Similarly, there are tasks and services that can be performed more efficiently by CSPs. These are often the back-end IT infrastructure that every business needs to have to operate, but does not relate to a health care or energy organization's core competencies. Often, however, back-end IT infrastructure is a CSP's core competency. Organizations should take a proactive approach in analyzing which tasks and services are appropriate to outsource to CSPs and which tasks and services must remain in-house.

b. Cloud Use in the Health Care and Energy Sectors

The Roundtable noted that the planned uses of the public cloud in the health care and energy sectors tend to be limited to ancillary services rather than core health care[37] or energy services. One might reasonably assume that this is driven by regulations that prevent organizations like health care providers from using the cloud, but that is not the case. As Phil Gordon, attorney at Littler Mendelson, noted, the Health Insurance Portability and Accountability Act ("HIPAA") and Health Information Technology for Economic and Clinical Health Act ("HITECH Act") do not specifically address the cloud. University of Colorado Law School Dean Phil Weiser pointed out that the tendency to avoid the cloud is more an artifact of status quo bias. It is likely that lack of regulation in this area that is specific to the implementation (cloud computing) that makes the cloud feel "different" and uncertain, an uncertainty that skews perception of risk in a risk-averse sector.[38]

c. Health Care Specific Themes

The perception of the cloud as an unsafe environment for sensitive data, combined with the perception that all data related to health care is highly sensitive, drives the assumption that the health care sector would be well advised to avoid the cloud no matter what the benefits of using the cloud may be. In reality, the variety of data types being processed by health care organizations, the customer demand for the convenience made available by the cloud, and the pressure for cost reductions in the health care sector will combine to drive smart health care companies towards opportunistic use of the cloud. Such opportunistic use involves private or community clouds in the health care sectors where organizations in other, less sensitive, sectors might be more comfortable using public clouds.

Health care is a heavily regulated sector with unique concerns, although such concerns often parallel concerns in other sectors. Health care also has particular demands from constituents outside of regulations. Finally, the use of cloud computing (or any other new tool) in health care has particular risks not present in most other industries.

i. Pressures to Use Cloud

[37] As Melodi Gates noted, some core health care functions, like electronic health records management systems, are using private or community clouds already.

[38] Gates also pointed out that the IT professionals often charged with making decisions to move to cloud providers are faced with a choice that can amount to outsourcing their own jobs or the jobs of many of their employees. Preserving one's own livelihood is a strong motivator.

Health care providers are feeling pressure to adopt cloud computing from several angles. Provisions of the Patient Protection and Affordable Care Act ("ACA")[39] and the HITECH Act[40] create pressures and incentives for health care providers to adopt EHRs. While larger providers typically have dedicated IT staff to support their systems, many small medical offices, as Gates noted, do not have even a single IT-trained person on staff but instead depend on part-time or contracted resources.

The ACA also limited the percentage of an insurer's budget that can be used for overhead.[41] This cost squeeze is going to force these health service providers to take a hard look at reducing costs through things like outsourcing IT tasks and services to CSPs. Additionally, as Bill Levis, the Consumer Counsel for Colorado, pointed out that, based on his previous experience as President of the Brain Injury Alliance of Colorado, health care is a choice. If one organization fails to be cost-competitive, customers can price shop and switch providers.

Finally, like many industries, there is a demand from data users for the accessibility and convenience that cloud computing can provide. Patrick Heim noted that physicians are demanding this sort of convenience and mobility. They are often more eager to adopt cloud computing than the organizations that employ them. Combined with health care consumers' demands for convenient access and transferability of their data, health care organizations are feeling increasing pressure to adopt cloud computing.

ii. Risks of Cloud

This fast access to electronic health data, as Dr. Larry Wolk, CEO of the Colorado Regional Health Information Organization ("CORHIO") noted, raises a common issue with all innovative changes to health care: the risk of committing malpractice. While clerical errors are nothing new in health care, the ways in which mistakes can be made, and the potential scale of those mistakes, multiply when documents are stored and transferred on the cloud rather than on paper. Until a standard of care is established with respect to how EHRs and medical data on the cloud are to be managed (and malpractice insurance providers clearly establish the bounds of coverage), health care providers will be understandably hesitant to adopt a new technology that may expose them to new and unknown risks.

Further, there are heightened privacy issues with respect to protected health information ("PHI") and medical records. While financial data is certainly sensitive and there is risk associated with other PHI, a leak of personally sensitive medical information can be much more difficult to rectify than other data leaks. Indeed, it can be challenging to make someone whole after personal financial information is stolen, but it is nearly impossible to make PHI that has been made public private again. For this reason, the risks are significant and difficult to measure even before considering the regulatory penalties.

---

[39] *See* KEY FEATURES OF THE AFFORDABLE CARE ACT, BY YEAR, http://www.healthcare.gov/law/timeline/full.html (last visited May 1, 2013).

[40] *See* EHR INCENTIVE PROGRAMS, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/ (last visited May 2, 2013).

[41] Patient Protection and Affordable Care Act, § 2718(b)(1)(A), 42 U.S.C. § 300gg-18 (2010). *See also* KEY FEATURES OF THE AFFORDABLE CARE ACT, BY YEAR, http://www.healthcare.gov/law/timeline/full.html (last visited May 1, 2013).

d. Energy Specific Themes

i. Energy Sector Background

The perception of the energy sector is that it has no incentive to be innovative and as a result, the cloud is not something it will adopt—risk or no risk. The reality is that there are areas of the energy sector that are incented to innovate. Furthermore, as the cloud becomes the new normal, the regulated entities within the energy sector will be expected to keep up.

The energy sector for the purposes of this Report can be broken down into two basic groups: regulated utilities and unregulated ancillary services.[42] Large portions of the energy sector operate as regulated monopolies with oversight from public utilities commissions ("PUCs"). These PUCs regulate the price a utility can charge customers for its services based on the utility's cost of doing business. The utility is allowed to include reasonable and prudent operating costs (i.e., employee costs such as salaries, pensions, benefits, etc.), fuel costs (i.e., coal or natural gas costs), and rate base costs (i.e., capital expenditures like power plants and office space),[43] as well as being entitled to earn a reasonable rate of return on the capital expenditures.[44]

The fact that these entities are regulated in this way is critical to understanding the incentives that influence how the energy sector approaches the adoption of CSPs for their IT infrastructure. Because these utilities are monopolies and do not have to fear competition from more efficient entities, they do not have the same incentive to seek cost-cutting solutions that an entity in a competitive industry would have. In fact, the utilities' incentives are driven by prior PUCs' decisions and assumptions about how future investments will be viewed by the Commissions. For example, capital expenditures that may be necessary to transition significant portions of IT infrastructure to CSPs run the risk of being deemed not reasonable and prudent by the PUC, preventing the utility from recouping its investment. As Wendy Moser, Vice President of Regulatory Services and Resource Planning at the Black Hills Corporation noted, it may not be prudent to depart from the status quo, especially if the initial capital investment costs are high and the benefits to customers are not easily documented. Likewise, if these changes *are* accepted as reasonable and prudent, and eventually reduce the need for future capital investments, the utility's rate base will decline rather than increase or remain constant, thus reducing the utility's earnings over time. As Wilkinson Barker Knauer attorney Ray Gifford succinctly noted, "If you innovate and win, you don't win and if you innovate and lose, you lose."

The energy sector, however, is not made up exclusively of these regulated monopolies. There are also unregulated ancillary services, some of which enable customers to have more insight into and control of their energy use. Services like Justin Segall's "Simple Energy" capture energy use information and allow customers to view and control their energy use. These kinds of businesses do have a clear incentive to innovate.

---

[42] This is, admittedly, a gross oversimplification of the landscape of the energy sector, but an analysis of the minutiae of regulations and entities in the energy sector is beyond the scope of this Report.

[43] Some PUCs have adopted the concept of "used and useful" to determine if capital expenditures should be allowed to be included in the rate base that utilities can recover in their billing rates. *See* Jersey Cent. Power & Light Co. v. Fed. Energy Reg. Comm'n 810 F.2d 1168, 1181 (D.C. Cir. 1987).

[44] Fed. Power Comm'n v. Hope Nat. Gas Co. 320 U.S. 591, 603 (1944).

ii. Energy-Specific Risks

There are two major risks with respect to cybersecurity that are specific to the energy sector: grid security, and privacy with respect to sensitive customer information. With respect to data and systems that relate to the power grid, there is no question that the highest level of security is necessary. In this instance, the only reasonable and prudent IT system is the safest one, and that may not be on the cloud. As Wendy Moser noted, because the costs of keeping the grid safe will almost certainly be considered reasonable and prudent, it is not a burden on the regulated utility to hire sophisticated security personnel like it would be in a competitive environment.

The other type of data is customer data. This includes information about energy use. The increasing use of smart meters allows for the creation of large amounts of this data. The data can be so detailed that it amounts to a window into the user's home.[45] While this data is still sensitive, it does not carry the significant security risks of the grid access data. Further, it is the kind of data to which many tech-savvy and energy-conscious consumers demand access.

iii. Energy-Specific Solutions

In the regulated energy sector, the nature of rate regulations has squeezed out much of the incentive to innovate. Provided PUCs adjust their rate case decisions in a way that welcomes or even incentivizes the adoption of CSPs for certain IT infrastructure functions among regulated utilities, then the approach becomes similar to the risk-management approach described above. The utilities must carefully examine what data and IT functions can be safely supported in the cloud. Those that require maximum security, like grid security issues, should be treated differently than more routine, lower-risk data and functions.

IV. Can the Cloud be Regulated?

Regulating the cloud is not simply a matter of creating a set of rules, handing them down to everyone who uses the cloud, and moving on to the next issue. The reality is, regulating the cloud, or more properly, regulating entities using the cloud, is an incredibly challenging endeavor that requires a level of flexibility and agility for which traditional command-and-control regulation is unfit.

In 1962, Everett Rogers introduced the concept of the technology adoption curve.[46] Rogers observed that new technology adoption looked like a bell curve with rate of technology adoption on the vertical axis and time on the horizontal axis. The curve shows a small percent of early adopters at the leading edge, the main bulk of the bell consisting of the early and late majority, and finally the trailing edge of the curve was the laggards.[47] If

[45] The information is so detailed that it has raised concerns that if law enforcement viewed such information, it would amount to a search under the Fourth Amendment and would require a warrant. *See* Smart Meters and the Fourth Amendment, IT LAW WIKI, http://itlaw.wikia.com/wiki/Smart_Meters_and_the_Fourth_Amendment (last visited May 3, 2013)

[46] EVERETT ROGERS, DIFFUSION OF INNOVATIONS (4th ed. 1995)

[47] *Id.*

Congressional lawmaking with respect to cloud technology were plotted on that same graph, it would be well behind even the laggards. The cloud has been adopted rapidly, and lawmakers and regulators have yet to catch up.

We have become accustomed to rapid innovation and adoption of new technologies. That, combined with the nature of the cloud as back-end technology that improves our user-facing applications without the user necessarily knowing that cloud computing is involved, leads to the perception that the cloud is a mature and robust technology. As Scott Shipman pointed out, it is important to remember that, in reality, the cloud is relatively new. As a new technology, many aspects of cloud computing, and surrounding technologies, institutions, and policy, are underdeveloped. In many senses, businesses are still figuring out exactly how to handle the Internet, which has been around for a generation. It should not be surprising, then, that they have not quite figured out how to handle cloud computing.

a. Current Regulations Addressing the Cloud

Cloud-specific regulation in the health care and energy sectors is uncommon. The bulk of the regulation that applies to cloud computing addresses privacy and security issues that exist irrespective of whether the data exists in cloud environments or exclusively on conventional computing systems.[48] As Mike Locatis, the Department of Homeland Security's Assistant Secretary for Cybersecurity and Communications, pointed out after the Roundtable, a number of developments will impact cybersecurity and cloud computing in a range of sectors, including health care and energy. Some of these changes are regulations, policy directives, and executive orders that address cybersecurity. Others, however, will seek to encourage the use of *more* cloud-based services into the government and private sector.

b. Recommendations for Regulating the Cloud

As lawmakers and regulators address the challenge of regulating cloud computing, they will run into the challenge that Ohio State University Law professor Peter Swire pointed out: if rule-makers create very specific rules with respect to cloud computing, the rules will be obsolete by the time they are published. If they create very general rules, they will be very difficult to interpret and likely cause confusion and potentially stagnation as organizations hesitate to be the first to test the boundaries of the new regulations. This tension seems to support the idea that governance of the cloud should be handled through mechanisms that are flexible enough to respond to the expected rapid changes. As one variation on regulating cloud computing directly, regulations can be aimed at what is being protected—the data—because mandating actions that are obsolete by the time they are in force would be both ineffective and wasteful.

Lawmakers already have experience creating laws that outline expectations of data privacy and penalties for violating such privacy. However, they lack the agility to make specific rules quickly enough to address each new technology. In light of this limitation, Gates pointed out that the regulations should focus on data collection, access and usage. Such regulation will put the onus on the users of the technology to ensure that they are

[48] The HITECH Act penalties described in note 35, *supra*, apply irrespective of whether the data resided on a cloud system or conventional system.

adapting as necessary to keep data safe. Defining sensitive data types, responsible parties, and penalties for breach of security may be the best that lawmakers can do. As noted in Section II.c., above, organizations should take an active risk management approach to cloud computing. So too should regulators, appropriately identifying risks based on the realities of cloud computing rather than the perceptions of it and putting in place rule and incentive structures that mitigate these risks in efficient and effective ways.

Conclusion

With transformative technologies, as with most things that suffer from a lack of understanding, there is a gap between the way the general public perceives the technology and reality of the technology. This gap persists, and leads to sub-optimal decisions, because the perception is the most readily available frame through which choices are viewed; understanding the reality of transformative technologies like cloud computing requires additional effort, which is often viewed as unjustifiable.[49] The challenge for today's business executives and IT professionals, especially those in heavily regulated sectors like health care and energy, is to understand the realities of cloud computing and take an active role in shaping the way their companies use the cloud. The cloud has the potential to be a very powerful tool, but like any tool, its value is decided by its use.

[49] *See* Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 SCIENCE 453, 458 (Jan. 30, 1981).

Appendix A
Cybersecurity and Cloud Computing Roundtable – Attendees

Dirk	Anderson	Coalfire
Erika	Bol	Colorado Dep't of Health Care Pol'y and Financing
Matt	Burns	University of Colorado
Dave	Campbell	Electric Alchemy
Bryan	Cunningham	Cunningham Partners
Doug	DePeppe	i2 IS Corporation
Charles	Duan	Silicon Flatirons Center
Melodi	Gates	Patton Boggs
Ray	Gifford	Wilkinson Barker Knauer
Phil	Gordon	Littler Mendelson
Dick	Grunwald	University of Colorado
Patrick	Heim	Salesforce.com
Todd	Hinnen	Perkins Coie
Harry	Horowitz	University of Colorado
Dave	Huberman	Webroot
Dan	Jones	University of Colorado
Micah	Jones	University of Colorado
Yianni	Lagos	Future of Privacy Forum
Larry	Levine	University of Colorado
Bill	Levis	Colorado Department of Regulatory Agencies
Mike	Locatis	Department of Homeland Security
Collin	Mariner	Tendril
Dayna	Matthew	University of Colorado
Wendy	Moser	Black Hills Corporation
Erin	O'Brien	CU-Denver Anschutz Medical Campus
Paul	Ohm	University of Colorado
Tarun	Reddy	Rally Software
David	Reed	University of Colorado
Chris	Roberts	One World Labs
Kristen	Russell	Governor's Office of Information Technology
Justin	Segall	Simple Energy
Scott	Shipman	eBay
Ashkan	Soltani	Independent Researcher and Consultant
Harry	Surden	University of Colorado
Peter	Swire	The Ohio State University
Omer	Tene	Israeli College of Management School of Law
Melissa	Van Buhler	University of Colorado
John	Verdi	Nat'l Telecomm. and Info. Admin.
Jay	Weber	One World Labs
Phil	Weiser	University of Colorado
Danny	Weitzner	Massachusetts Institute of Technology
Dick	Williams	Webroot
Larry	Wolk	CORHIO