Making the Decision to Contract for Cloud Services:
Managing the Risk of an Extreme Form of IT Outsourcing

Eric K. Clemons | The Wharton School | clemons@wharton.upenn.edu
Yuanyuan Chen | National University of Singapore | discy@nus.edu.sg

Abstract

Obtaining cloud computing services can be viewed as a form of outsourcing, and as such it shares the essential risk profile of all outsourcing contracts concerning opportunistic behavior, shirking, poaching, and opportunistic renegotiation. Developing cloud computing is also an advanced technological development effort, and as such it shares all of the risks of large and uncertain development efforts and the essential risk profile of all development efforts where for a variety of reasons success cannot be ensured, including functionality, political, project, technical, and financial risks. Since E-Government services are almost by definition delivered online, rather than by visiting government service locations or through paper-based interaction, they would appear an obvious candidate for cloud-based delivery; consequently the risks of cloud-based delivery services are of critical interest to the safe execution of numerous E-Government missions. This paper focuses on understanding the risks, both through understanding standards and understanding contracting for cloud services. Standards for cloud computing may reduce many of the risks of opportunistic behavior on the part of vendors. Standards efforts cannot mitigate most of the development risks of cloud computing; no amount of legislation or standardization can make it possible for firms to do that which they could not have done, or that which is indeed algorithmically or computationally infeasible.

Keywords: Cloud Computing, Cloud Contracting, Cloud Standards, E-Government, Outsourcing Risks Associated with Cloud Computing.

1. Introduction

This paper is about sourcing cloud computing services. More precisely, it is about understanding the risks of cloud computing, understanding the role of standards in managing those risks, and understanding how these risks can be managed through contracting. Outsourcing is by now a well-studied subject, but cloud computing is such an extreme form of outsourcing that it appears to raise new concerns. We suggest that since cloud computing is a form of outsourcing, the elements that contribute to its risk profile are the same as those associated with any other form of outsourcing. Likewise, cloud computing is also an aggressive new advance in online, web-based computing, and as an advanced technology development effort, the elements that contribute to its risk profile will be the same as those associated with other advanced development efforts. The sources of risks may be different from those associated with previous, and now better understood, outsourcing decisions; this paper attempts to clarify them so that they can be understood, assessed, and managed or mitigated.

Since the very essence of E-Government is the online provision of services in a cost-effective and scalable manner, it is likely that E-Government will be increasingly dependent upon outsourced cloud computing for deployment of its services. Additionally, for reasons that we will describe in more detail below, the issues that raise concerns in commercial users of cloud services will be even more significant a cause for concern in E-Government. But the importance to E-Government of the issues on which we are focusing is clear even from a casual inspection of the 2010 HICSS call for papers. The mini-track on E-Government Infrastructure and Interoperability requests papers on interoperability standards, principles and frameworks

operations are transferred to the cloud vendor, but with software as a service and platform as a service, much of software development and even control of the platform that enables software development are also transferred to the cloud vendor. Cloud computing adoption is an increasing trend in IT spending. In the first half year of 2009, the adoption of cloud computing jumped 320 percent [43]. Spending on cloud computing is expected to reach of 30% to 40% of IT budgets in the next three years [4].

Cloud computing is attractive to governments around the world as well as to corporations. U.S. Government spending on cloud computing service is expected to grow from $277 million in 2008 to $792 million annually by 2013, with a growth rate of approximately 30 percent annually [21]. The General Services Administration (GSA) contracted out the U.S. federal government’s primary e-government portals — USA.gov — to a private cloud computing service provider in the summer of 2009. The shift to the cloud is also taking place in governments around the world. For instance, in Japan, the national government is developing a private cloud environment that would eventually host all of the Japanese government’s computing [28]. In the European Union, the European Commission is undertaking a major initiative to create a cloud-based IT infrastructure in EU member states [15].

In order to make cost-effective cloud computing decisions that adequately protect against risk it is necessary to understand what cloud computing is, what its risk profile is now and will be in the near term, and how standards affect those risks now and in the near term. Then, and only then, can firms or governmental bodies accurately assess their objectives and strategy for cloud computing.

The structure of this paper is as follows: Section 2 reviews what cloud computing is and why it has become attractive now. Sections 3 reviews the risks associated with cloud computing in the context of the risks of traditional IT outsourcing. We discuss the unique legal risks associated with cloud computing in Section 4. We focus on how standards can reduce the risk profile of cloud computing and summarize the current status of standards in Section 5 and 6. In Section 7, we discuss how to design major components of cloud contracts to reduce risks in cloud computing. We conclude the paper and briefly discuss the future research in Section 8.

2. What cloud computing is and why it is emerging now

2.1. A description of cloud computing

The first, and perhaps most basic, component of cloud computing is Infrastructure as a Service (IaaS). IaaS has its roots in the virtualization technology of the first decade of the 21st century. Rather than specifically assign applications to machines, the entire computing facility of a firm is viewed as a collection of servers, running a collection of virtual machines, on which jobs could be assigned as needed. The next logical extension is to have remote server farms provide virtualization services rather than obtaining them in-house. The larger the vendor, the smaller the variance in expected total demand. This means that cloud computing offers the most efficient allocation of computing resources, even for the largest and most technologically intense users.

The cloud’s second component is Software as a Service (SaaS). SaaS entails replacing purchase or lease of software, operated on the client’s site, with pay per usage (person-hour, transaction volume, or other measure) operated in the cloud or on the vendor’s site [42]. The software envisioned in SaaS may be core to a business’s operations, encompassing HR, accounting, ERP, or other essential processes.

Perhaps more novel, the third element is Platform as a Service (PaaS). In PaaS, vendors provide a propriety development platform, in addition to infrastructure and software. While PaaS may greatly accelerate software development and deployment, it may also lock users into the services of a specific vendor, since vendors’ development platforms will differ, and hence software suites developed on one cloud vendor’s platform may or may not operate properly in the environment of other vendors.

These elements, IaaS, SaaS, and PaaS, when combined with online Internet access, provide the technology needed to generate cloud computing.

2.2 Why the cloud is interesting now

Many of the elements of cloud computing have been available for some time but numerous factors combine to make cloud computing attractive today. In brief, the cloud is emerging because it now promises to be cheaper and it is now possible to implement the cloud.

The cost of hardware is no longer a significant fraction of expense in most computing installations, but personnel costs still keep the costs of installations high. The cost of systems administration personnel (Sys Admins) greatly exceeds the cost of the servers they manage in most enterprises. Cloud computing enables a firm to pay the fully loaded costs — hard-
ware, power, heating and cooling — only for the time they actually require their machines, which greatly rewards load leveling through cloud computing. The massive reduction in the expense of Sys Admins enabled by cloud computing may be even more important. A small shop may require a Sys Admin for 10 servers. A large shop may be able to use one Sys Admin for every 1,400 servers. Huge and highly automated operations like Google’s or Amazon’s cloud services claim to be able to leverage one Sys Admin for every 10,000 or even every 100,000 servers, with claims that still further improvement is possible. Cloud computing also changes the economics of hardware deployment by reducing the secondary and indirect expense associated with idle capacity and by automating server management. In brief, cloud computing offers even the smallest firms significant economies of scale in all aspects of their hardware expenditures, reducing both capital and operating expenses.

SaaS allows many firms to avoid software development entirely and to use standard packages. While claims that SaaS eliminates barriers to entry for small firms, or eliminates delays in developing and rolling out support services, or eliminate the cost advantages of large firms [42], SaaS does provide motivation for the move to the cloud for organizations with needs that are similar to the needs of others. More novel is the fact that PaaS changes the way firms develop their own service, greatly accelerating software development and reducing software development expenditures. While SaaS allows firms to operate without developing unique software, PaaS promises to provide specialized development platforms that make custom development faster, cheaper, and more reliable. Once again, these effects will be most significant for the smallest firms.

IaaS promises to reduce hardware costs and data center operations personnel and SaaS and PaaS promise to reduce software costs. For a more complete treatment of the claimed benefits, see [18].

Two trends, both well advanced, support cloud computing by ensuring that most applications already run on a common infrastructure.

- The X86 architecture has been almost universally adopted for processors, from smaller servers deployed in massive server farms as well as the largest corporate mainframes, and most run Linux or Microsoft operating systems, with some form of virtualization hypervisor.
- Likewise, we see the nearly universal penetration of high-speed Internet, based on LANs and WANs, and increasingly on WiFi remote access as well.

Interestingly, the element of cloud computing that most captured the popular imagination is the idea that since everything is online somewhere, everything is in the cloud, and since everything is in the cloud, everything is available through cloud computing. However, two elements will be essential before everything present in the cloud could actually be available in the cloud.

- The first is true semantic access. Database management went a long way towards allowing information to be accessed based on its description (the essence of relational query languages) rather than by its location. URLs and hyperlinks allow users to access anything for which they know the address (assuming they have access privileges) but they do not allow the user to find and integrate all information that resides online anywhere.
- The second is interoperability and cross-cloud integration. Individual clouds are at present more like separate islands of related access, or even separate archipelagos, but scarcely support full interoperability. Each cloud has its own footprint, but at present clouds are separate and their footprints vary greatly in size.

3. Traditional outsourcing risks associated with cloud computing

The risks of contracting for cloud computing include the standard risks associated with any form of outsourcing. Surveys of users indicate that concerns for these risks are quite salient [18]:

- Users are concerned that they will be locked in, resulting in higher costs.
- Users are concerned that they will lose control over essential data or over essential proprietary expertise.
- Users are concerned with under performance of critical tasks, especially those associated with protecting their data security and data integrity.

Each of these translates directly into one of the standard risks associated with traditional outsourcing.

3.1. Outsourcing opportunism risks

Outsourcing opportunism risks are generally
seen to have their roots in three forms of deliberate, self-serving vendor behavior. These were initially studied for decades by economists, who were concerned with the risks associated with any form of contracting. They have more recently, over the course of the past two decades, been used by information systems specialists, to study the risks of any form of information technology outsourcing.

- **Shirking and deliberate under performance** [1, 2, 3, 5, 716]

- **Poaching and the theft of intellectual property, proprietary software, critical confidential data** [2, 7, 8, 20, 23, 35]

- **Opportunistic repricing, client lock-in, and vendor hold-up** [2, 3, 9, 10, 26, 37, 38]

Shirking involves a vendor’s deliberate under-performance, while claiming full payment for services, and is enabled by information asymmetries. If the client were able to fully observe both vendor output and vendor effort, shirking would not be possible. The forms of shirking that will be possible in cloud computing contracts include (1) deliberate under-investment in server capability, creating slow-downs that can be blamed on the network rather than the service provider; (2) deliberate under-investment in back-up, dynamic firewall monitoring, and other data quality services that can detected only in the event of loss of data or a breach of security, and (3) under investment in excess or spare capacity, which will be detected only in the event of highly correlated demand, due to anything from market crises, major shopping holidays, or focused denial of service attacks, which again would be undetected until the critical events occurred. It’s not clear how corporations would deal with digital brown-outs caused by unanticipated peak demand on cloud computing, caused by events that lead to spikes in transactions.

Poaching includes a vendor’s misuse of data or of programs residing on the vendor’s site. It can entail making critical resources available to their owner’s direct competitors, or providing them to vendors who will then do so; clearly, poaching entails the misuse of resources provided under contract, their use outside the terms of that contract, their use for the gain of the vendor, and their use in ways that harms the client. Other uses are less direct or less obvious, such as using resources simply to let a competitor of the client anticipate the client’s plan, or even to allow the vendor to anticipate the client’s renegotiation strategy with the vendor itself.

While security and privacy are concerns for corporations, the misuse of private data may be even greater concerns for users of E-Government services. Having a bank ID compromised can lead to theft, but most financial loss due to compromised bank security is the responsibility of the financial institution at fault; individuals can be massively inconvenienced, but their financial exposure is limited. In contrast, having an E-Government ID compromised can involve the loss of control over almost all aspects of an individual’s most personal information; this can lead to full identity theft, which is widely acknowledged to be a problem if tax identifiers or similar information is compromised [24, 27].

Opportunistic renegotiation is perhaps the greatest risk traditionally associated with outsourcing, and with so much outsourced to a single party it may be even greater in the cloud environment. While IaaS can be made reasonably safe, the other levels of cloud service provision are extremely vulnerable to vendor lock-in and subsequent opportunistic repricing. SaaS and PaaS create more risk. To the extent that a client has developed unique applications based on a unique vendor platform, the client can no longer move his suite of applications to another vendor. Software developed on the Salesforce.com platform cannot readily be moved to a Google or Amazon cloud software development platform because it will be dependent upon calls to applications or to data that will not be made available. That suggests the lack of interoperability at the higher levels of SaaS and PaaS create significant risks for the client due to the great possibility of opportunistic behavior by the vendor over time. Vendor lock-in is an issue that has been widely studied in the context of corporate buyers and government contractors [22, 25, 34], and is likely to become a greater concern as E-Government moves less experienced government organizations into the procurement of online services.

### 3.2. Technology development risks

Complex development projects always create operational risks, due to the technical and operational limitations of the development effort. These risks are quite independent of risks that are motivated by deliberate opportunism by the vendor. Since the opportunism risks associated with outsourcing are due to differences in incentives between client and vendor they can often be managed or mitigated by contract design. In contrast, the development risks associated with complex deployment of novel technologies, or technologies in novel combinations, are difficult to manage and unlikely to be managed solely by contractual mechanisms.

The list of risks is easier to identify than to manage [12, and again the types of risks have remained largely unchanged for decades, although the
specific sources of these risks have always varied from one application domain to another.

- **Functionality Risk** — Functionality risks arise when we do not know what systems will be required to do, or what they will be required to do over time as users and their requirements evolve [5, 33]. We do not yet know entirely what capabilities will be needed in the cloud over the coming years. In particular, we do not know to what extent SaaS and PaaS will predominate, and therefore we do not know to what extent it will be increasingly difficult to integrate new applications with the existing legacy systems of the organization developed without proprietary PaaS. Likewise, we do not know what will be required to develop applications developed in different clouds as a result of corporate mergers or restructuring activities. In addition, we do not yet know what forms of “data citizenship” will be required or how emerging legislation will emerge on what data can and cannot be stored outside a country (e.g. France or Singapore) or outside an economic zone (e.g., the European Union).

- **Political Risk** — Political risks arise when members of the organization have reason to resist the proposed new development effort, most frequently involve job security, status, or compensation. The move to cloud will, over time, render most of the local Sys Admin personnel redundant, and likewise may greatly reduce the number of in-house software developers required. These employees will ultimately become unnecessary, but many of the best may leave for alternative employment long before the client firm is ready to let them go. All firms must now be careful to avoid actions that would cause their best staff to leave before the firms are able to replace them in the cloud.

- **Project Risk** — Project risks arise when the combination of technologies, or the scope of the development efforts, exceed the ability of developers to manage the implementation, to ensure adequate testing and thereby ensure adequate quality, or to ensure timely completion [12]. We can legitimately ask if any of the parties, either clients or vendors, really know how to perform the porting of applications to the cloud. Do they know how to ensure that the suite of applications will run properly while some are on the client’s site and some are in the cloud, and while some have been developed with traditional application development methodologies and some have been developed with the cloud vendor’s proprietary platform?

- **Technical Risk** — Technical risks arise when projects exceed the capabilities hardware or software technology, or exceed the skills of the best available developers [31, 33]. We can ask if there are unsolved technical problems, involving security and privacy, or involving integration of applications developed on the client’s site with those on the vendor’s site, that could make implementation of cloud computing more difficult than anticipated. Perhaps the only truly unbreakable security systems involve quantum computing, and these appear to be years or even decades away from widespread implementation. Again, while firms are concerned with unsolved problems in implementing secure cloud computing, these concerns may be even greater for E-Government service providers because of the greater risk of identity theft.

- **Financial Risk** — Financial risks occur when projects fail to deliver expected benefits. How large are the benefits from cloud computing? For some small or medium enterprises, the benefits may be very large, since they will get great reductions in operating expense from the greater economies of scale on systems administration, and because they are too small to benefit from load leveling opportunities without migrating to the cloud. Likewise, for new entrants, either small firms, or small new business units within firms, the cloud and the promise of SaaS may offer faster market entry. For established firms, the benefits from IaaS and SaaS may be smaller than promised.

4. New cross border legal risks

4.1. Cross border litigation

Cross border litigation is always problematic. Transactions on the cloud can potentially span many national borders, with a client in one nation, a vendor in another, the cloud data center in a third, and the Internet service provider spanning numerous others. When cross-border wrongs (torts) are committed they lead to cross-national litigation. Several elements of cloud computing may make cross border litigation in the cloud setting even more problematic.

- **Ambiguous performance measures may make it hard to detect problems or to assign responsibility to the guilty party**: If the end user’s service degrades is this the fault of the vendor, the net between the vendor and the client, a third party provider of software, or the user client’s own service measurement? The cloud will require standard and transparent measures of service level agreements and of transparent observation of the quality of all
aspects and all components of service delivery.

- **Problems with misappropriation of data or programs:** Litigation must occur in a jurisdiction with a legal system with strong respect for the rights of the owners of intellectual property.
- **Problems with valuation:** If damages are assessed, the client needs a legal system that will assess damages commensurate with damage incurred in the client’s country and with client’s norms.

The first and most fundamental issue is in what circumstances does a court have jurisdiction over a foreign defendant alleged to have committed a wrong in the cloud? The next issue is whether each contract party (either cloud vendor or client) can select the forum and jurisdiction when drafting a cloud contract, and indeed whether either party’s home jurisdiction — either plaintiff’s or defendant — will honor the contract’s specification of jurisdiction if it is believed to be biased and unfavorable to the local party?

### 4.2. Data citizenship and data residence

There is increasing concern in the US, the EU, Singapore, and other venues, about where data on their citizens can be stored and accessed (see, for example, Section 505 of the USA Patriot Act, or the EU Data Protection Directive 95/46/EC). Some cloud vendors do not provide locations in all venues, and some do not permit clients to specify the location of their data. Some have due diligence procedures that require multiple copies to ensure security, or caching to ensure performance, and it is not yet clear how users can specify data locations or can ensure that their specifications are followed.

Governmental bodies at national, state, and local levels may prohibit cloud providers from storing government data out of country boundary to avoid the risks that their citizens’ data will be subject to review by other governments. There is little doubt that restrictions on the location of data will remain a factor in E-Government and little doubt that these restrictions will increase [29, 40]. For example, the Canadian national government recently asked government agencies not to use computers operating within United States borders because the data may under US surveillance according to the Patriot Act. Increasing governmental concerns about data location may impede the shift to cloud-based E-Government.

### 5. The role of standards in reducing the risks of cloud computing

#### 5.1. The impact of standards on shirking poaching and opportunistic renegotiation

Shirking is heavily dependent upon information asymmetry [1, 2]. If standards ensure that the vendor’s behavior is observable, if performance measures are clear, transparent, and unambiguous, and if the nature of every performance lapse can be unambiguously traced either to vendor failure or external failure, then service level agreements can be enforced and one aspect of shirking is no longer a cause for concern. If standards likewise ensure that security, integrity, and data backup procedures are transparent and routinely monitored, then another aspect of shirking associated with cloud computing can be managed. The third and final element, reserve capacity, almost requires government regulation, just as banks and insurance companies are required to maintain adequate financial reserves; competitive markets do not adequately reward the maintaining of idle or reserve capacity.

Like shirking, poaching is a problem only if it cannot be detected and punished. With adequate standards for the storage and subsequent audit of the full history of data access it should be possible to ensure that online resources — online programs and data — are not accessed by third parties. It is less clear how standards can ensure that data copied for archiving and security purposes are not abused.

Opportunistic renegotiation is only possible when the client’s initial commitment to a vendor becomes unbreakable over time [9, 10, 37, 38, 39], allowing the vendor almost unlimited opportunities for repricing in the future. Standards for the transfer of applications and of data from one vendor to another would ensure that holdup does not become a problem. The more a client is dependent upon the offerings of a specific vendor the more entangled the client becomes and the greater the vendor’s freedom to engage in opportunistic behavior. In particular, proprietary SaaS programs, with proprietary data formats, make transfer back to the client’s own shop difficult. Even applications developed by the client’s own personnel, but developed on a vendor’s proprietary PaaS platform development offerings, may be impossible to port to a new vendor, which contributes to lock-in and the possibility of holdup and opportunistic repricing.

It is difficult for anyone who has not lived through a major conversion effort (like the mid 1960s conversion from the IBM 1401/1410/7010 architecture to the IBM 360 architecture) to realize how difficult porting an entire application base can be. Likewise, it is difficult for anyone who did not observe the impact that Microsoft’s slightly incompatible standard for Java had on Sun and Netscape to understand how greatly even a small difference in
5.2. Impact of standards on functionality
risk, technical risk, and financial risk

It’s not immediately obvious how standards can reduce most of the risks associated with the development of cloud ventures. Standards might help make it clear what the cloud would and would not be able to provide, reducing the functionality risk associated with reliance upon the cloud. Standards will not help deal with the political risk created by key personnel who know that they will soon be made redundant, and who leave before the organization is able to deal with their departure. Standards, properly designed for interoperability among cloud vendors, may help ensure interoperability between applications on the cloud and applications on a client’s site. This would help reduce the project risk associated with phased transition from client-based applications to cloud-based applications, and would help clients manage shops that included the integration of both client-based and cloud-based applications. While standards themselves will not address the problems caused by technical implementation difficulties within the cloud, by helping to define what is required, standards may reduce the technical risks of vendors’ efforts to implement their cloud offerings. Likewise, standards themselves will not reduce the financial risks associated with cloud-based implementation. However, to the extent that standards reduce the risks associated with using SaaS and PaaS, standards may favor a move to cloud computing.

6. Status of standards activities

Standards activities are under way in most major technologically advanced nations. There are activities led by governmental bodies, NGOs, and industry associations. The U.S. National Institute of Standards and Technology (NIST) is working on the definition of cloud computing. In addition to participating in these activities, leading technology vendors — both current cloud vendors and outsourcing firms that hope to gain significant cloud market share — are fighting in what can best be called the cloud standard wars [19]. IBM joined an alliance with dozens of companies including AMD, Cisco, Fujitsu, HP, and Intel to form the Open Cloud Standards Incubator Leadership Board. IBM wants an open standard for its own competitive reasons, as does Microsoft. In contrast, other cloud pioneers, including well-established vendors such as Google and Salesforce.com, seem opposed to the open standards [17]. It appears that their competitive strategies will be advanced by differentiated offerings and closed cloud platforms.

Industry associations are playing key roles and making progress in setting cloud standards. For example, The Storage Networking Industry Association (SNIA) has approved a standard for the Cloud Data Management Interface (CDMI) as a SNIA architecture standard in the spring of 2010⁶, and the Association for Retail Technology Standards (ARTS) provides guidelines for private clouds.

Paradoxically, despite the enormous concerns of potential cloud customers for lock-in, hold-up, and opportunistic repricing, almost no significant standardization efforts under way today are aimed at ensuring interoperability or portability among competing cloud vendors.

The increasing importance of cloud computing will force more governments to become actively engaged in standards, to protect their firms, to protect citizens interacting with corporations, and to protect citizens interacting with E-Government services. Trust in E-Government requires trust in the quality of the network and its services [13, 14, 32, 34], which will of necessity be related to the standards adopted. Indeed some governments, like Japan, and the UK, have done so [36, 41]. Anecdotal evidence suggests that at present governments are more concerned with the competitive implications of cloud regulations than with the safety of their networks or their citizens.

7. Major components of cloud computing contracts

Another way to reduce risks in cloud computing is to design contracts that carefully address the specific risks of cloud-based sourcing. From the client’s perspective, firms should fully understand three general dimensions of cloud contracts: performance (including both service level requirements for normal operations and data transfer rights upon termination), security (including data citizenship and data residence (i.e., where data may be stored and where it may be accessed)), and legal recourse:

- **Performance**: Contracts should have a clear definition of service level requirements on (1) availability of services including uptime, support time, and average and worst case response time; (2) system and network capacity, including ability to scale to meet unanticipated demand and time to respond to requests for capacity increases; (3) application quality and reliability, in the case of SaaS; and (4) stability (backwards compatibility) and quality (lack of errors) in the case of PaaS. The contract should specify how these will be measured, what data the vendor will provide to support measures, and how the client will verify the data provided, as well as penalties for service failure. The contract should also specify the disaster recovery plan. The terms of current contracts are often unacceptably disadvantageous to the client; for example, most cloud contracts grant the vendor the right to terminate client’s right to get access to data at any time for any reason [41].

- **Security**: The second dimension addresses security, which relates to data ownership and access right, and is a form of protection separate and distinct from disaster recovery plans. Contracts should specify the client’s ownership of data on the cloud and limit vendor’s access rights to those absolutely necessary to provide services for the client. In addition, the contract should clearly specify the scope of data security protection and the penalty and the responsibility and liability of vendors in the event that a security breach does occur. In many current cloud contracts, data security is not guaranteed; the vendor is exempted from many of the responsibilities as a joint provider of the cloud service (e.g., Amazon Web Service). Another important contract clause, serves to regulate what happen to the data after service termination [34, 41].

- **Legal recourse**: Legal recourse is related to how parties resolve disputes. Legal recourse covers two areas: legal claim and evidence collection, and jurisdiction and forum selection. The right to file legal claims and rights to evidence collection should also be covered in the contract for cloud services. Jurisdiction and forum selection refers to the contract clause(s) that determines how the parties will initiate any litigation resulting from the contract and which forum or jurisdiction will have authority. Cloud vendors always specify a particular court in their preferred jurisdiction to hear any litigation matters.

8. Conclusions and future research

Our conclusions are direct and straightforward:

- Cloud computing is a form of outsourcing, and it shares the essential risk profile of all outsourcing contracts concerning opportunistic behavior.

- Standards for cloud computing may reduce many of the risks of opportunistic behavior on the part of vendors. Despite the enormous concerns of potential cloud customers for lock-in, hold-up, and opportunistic repricing, almost no significant standardization efforts under way today are aimed at ensuring interoperability or portability.

- Cloud computing is an advanced technological development effort and shares the risks of large and uncertain development efforts. We do not yet know how some of these risks can be addressed.

- Standards efforts cannot mitigate most of the development risks of cloud computing. No amount of legislation or standardization can make it possible for firms to do that which they could not have done, or that which is indeed algorithmically or computationally infeasible.

- A good outsourcing contract is probably even more important in the cloud computing environment than it is for traditional outsourcing. Given the magnitude of the losses that can occur due to loss of intellectual property or breach of security, it’s also essential that the contract protect the client’s rights to litigate in a forum that is likely to be fair and unbiased, and likely provide fair and accurate valu-
ation of any losses. The best contract, of course, is meaningless if the vendor is both unable to perform in accordance with the terms of the contract and unable to make adequate restitution. In cloud computing, like any other critical form of outsourcing, the vendor must be both technically and financially qualified.

Future research will address (1) the evolving status of standards, their ability to protect clients, especially from risks caused by limited interoperability, (2) the contracting mechanisms available to manage risks as standards evolve; (3) the remaining risks facing E-Government, particular concerning data citizenship, data residence, and trust; and (4) business models being pursued by various vendors. Current experience (e.g., Capital One [11]) and the theory of contestable markets [6] both suggest that in the absence of switching costs or other market imperfections, it is difficult to over-charge customers to compensate for losses incurred during earlier, business development activities. And yet all cloud computing vendors currently have business models based upon under-charging for services. Some vendors may expect to earn super-normal profits on hardware, or on enterprise software, or on mining their clients’ corporate data, or on overcharging later after clients are locked in due to lack of standards, but all must have some expectation of earning profits later. Furthermore, if vendors’ estimates of cost reductions are wrong, as some readers of this paper have suggested, then these vendors will be even more driven to overcharge clients to the extent enabled by lock-in and lack of interoperability.

9. References

M-leads-call-for-open-cloud-standard.html.


We acknowledge the assistance of Ms. Naoko Kurata of Unisys Nihon, who helped with the research on standards.