Municipalities in a Cloud?
Cloud Computing Implications for Municipalities

Colin Grant[1]

OVERVIEW

This paper suggests that municipal interest in Cloud computing should be more or less the same as interest in any other Information Technology (IT) option. The Cloud highlights the broad and complex range of IT options available to consumers in the market today. The Cloud also reminds us of the general need for municipalities to consider IT resources as an integral part of municipal strategic planning, and to make IT decisions with the input of City Clerks and IT lawyers.

The main benefit of the Cloud derives from its economy of scale through outsourcing and sharing resources; however, satisfying the responsibility to protect private information remains a significant barrier to many Cloud solutions, as municipalities cannot outsource the responsibility for protecting information.

This paper will review: 1) what the Cloud is supposed to be and why it is generating so much attention; 2) what the Cloud is and is it really so different from other IT options and 3) review the risks and challenges of Cloud solutions, with some practical strategies for municipalities to assess whether a Cloud solution may be the right option in appropriate circumstances.

1. THE "BUZZ" ABOUT THE CLOUD

1.1 Definition of the Cloud

The term "Cloud" is used as a metaphor for the Internet, based on the Cloud drawing used in the past to represent the telephone network, and later to depict the Internet in

[1] The opinions expressed in this paper are personal.

computer network diagrams as an abstraction of the underlying infrastructure it represents.[2]

There are many definitions of "Cloud computing" in the literature on this subject. Generally, Cloud computing refers to the use of remote computer networks or resources operated by third parties to process, store and manage data.

The definition developed by the U.S. National Institute of Standards and Technology (NIST)[3] and cited by the Office of the Privacy Commissioner of Canada[4] is:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of essential characteristics, deployment models, and various service models.

A leading provider or "Cloud services" defines it a little bit differently:

> "Cloud computing is a broad term, but in our view maps to methods that deliver infrastructure, services, and software via the network on demand, and at scale. Cloud is based on a foundation of virtualization, in which pools of (virtualized) resources are dynamically organized for the benefit of software applications and services. This will change the way that applications are written and delivered."[5]

[2] Wikipedia, the free encyclopedia

[3] National Institute of Standards and Technology, "The NIST Definition of Cloud Computing" document posted October 2009, http://csrc.nist.gov/groups/SNS/Cloud-computing/.

[4] Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing (Draft)

[5] "Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing," CISCO White Paper, November 2009

I like the non-technical definition provided by Wikipedia:

> Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).

1.2 Analogy: the Cloud as a Utility

I find the above Wikipedia definition helpful because of the analogy of the "Cloud" to a "utility." As municipal lawyers, a public "utility" is a concept with which we are familiar.

The Federal Chief Information Officer for the United States, (from all accounts a champion of Cloud solutions) builds on the concept of the Cloud as a utility in his paper on The State of Public Sector Cloud Computing, as follows:

> There was a time when every household, town, farm or village had its own water well. Today, shared public utilities give us access to clean water by simply turning on the tap; Cloud computing works in a similar fashion. Just like the water from the tap in your kitchen, Cloud computing services can be turned on or off quickly as needed. Like the water company, there is a team of dedicated professionals making sure the service provided is safe and available on a 24/7 basis. Best of all, when the tap isn't on, not only are you saving water, but you aren't paying for the resources you don't currently need.[6]

The "utility" analogy" is also used in the book "The Big Switch: Rewiring the World, from Edison to Google":

> "In the years ahead, more and more of the information-processing tasks that we rely on, at home and at work, will be handled by big data centers located out on the Internet. The nature and economics of computing will change as dramatically

[6] "State of Public Sector Cloud Computing," May 20, 2010, Vivek Kundra, U.S. Federal Chief Information Officer

> as the nature and economics of mechanical power changed with the rise of electric utilities in the early years of the last century. The consequences for society—for the way we live, work, learn, communicate, entertain ourselves, and even think—promise to be equally profound. If the electric dynamo was the machine that fashioned twentieth-century society—that made us who we are—the information dynamo is the machine that will fashion the new society of the twenty-first century."[7]

Thus, rather than thinking about IT as an exercise in asset ownership, we can think about IT as a utility. We will discuss later in the paper that migration to the Cloud may be easier said than done. The point for now is that Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with water utilities and the electricity grid, where end-users consume water and power without having to understand the component devices or infrastructure required to provide the services.

1.3 Why is the Cloud generating so much interest?

Cloud computing fills our seemingly perpetual need for more and better IT services.

Cloud computing providers deliver applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location. Thus, the Cloud is one way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software.

[7] *The Big Switch: Rewiring the World, from Edison to Google*, N. Carr, W.W. Norton & Co., 2008.

Proponents of the Cloud refer to a bounty of benefits.[8] First and foremost, this paper suggests that the main benefit of Cloud computing are the economies of scale that the Cloud can create, from which a number of other benefits derive. The Cloud provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources assigned and reassigned according to consumer demand. Because resources are pooled, each user community does not need to have its own dedicated IT infrastructure. Communities can share computing resources, leading to higher rates of use on fewer servers and fewer dedicated staff.

As we will see later in the paper, one concern is the location independence of the Cloud; the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center).

Nevertheless, in theory the benefits that derive from the economies of scale of Cloud computing include:

> *Cost effective*: Cloud computing is a pay-as-you-go approach to IT, in which a low initial investment is required to get going. Additional investment is incurred as system use increases and costs can decrease if usage decreases.
>
> *Flexible:* IT departments with fluctuations in user load do not have to scramble to secure additional hardware and software. With Cloud computing, they can add and subtract capacity as its network load dictates, and pay only for what they use. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, and capabilities may be rapidly scale up or down.
>
> *Consistent Service*: We have all experienced network outages. Cloud computing can offer a higher level of service and reliability, and an immediate response to

[8] For example see State of Public Sector Cloud Computing," May 20, 2010, Vivek Kundra, U.S. Federal Chief Information Officer

emergency situations (although note that even the Cloud is not immune from outages[9]).

Broad network access: Who knows what the workplace will look like in ten years. Cloud capabilities are available over the network and accessed through standard mechanisms that promote use by the client preferred IT platforms (e.g., laptops smart phones, PDAs).

2. REALITY CHECK ON THE CLOUD

The uniqueness of the concept of Cloud computing has been a subject of dispute. Much of the technology and infrastructure of "the Cloud" was already in place long before the term itself existed.[10]

2.1 Technically speaking: What is the Cloud?

a) Cloud Deployment models

What is considered to be "the Cloud" can also be considered as four different Clouds. In IT jargon, what I call the four different Clouds, are commonly referred to as the four Cloud deployment models, as follows:

1) *Public*: Cloud infrastructure made available to general public

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

[9] For example, Gmail outages in 2008 and 2009 were the subject of an article in pcworld www.pcworld.com/article/160153/gmail_outage_marks_sixth_downtime_in_eight_months

[10] For example, Dell applied to trademark the term "Cloud computing" in the United States, but received a formal rejection of its trademark application, according to "Inside Trademarks", March 24, 2010

2) *Community*: shared Cloud infrastructure shared that supports specific community with shared concerns

   Community 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 premises or off premises.

3) *Private*: Cloud infrastructure operated solely for an organization

   Private Cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party and may exist on premises or off premises.

4) *Hybrid*: Cloud infrastructure comprised of two or more Clouds that remain unique entities but have data or application portability

   Hybrid Cloud infrastructure is a composition of two or more Clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability or load-balancing between Clouds.

b) Cloud Service Models

As a Cloud client one can access Cloud services through any computer hardware and/or computer software (e.g. computers, smart phones). Once an internet protocol connection is established among several computers, it is possible to share services within any one of three "layers" of service.[11]

[11] The servers layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of Cloud services, including multi-core processors, Cloud-specific operating systems and combined offerings.

The three service delivery models are commonly referred to in the IT industry with the jargon SaaS, PaaS, and IaaS:

1) *Application* – Cloud Software as a Service (SaaS)

   Cloud application services or "Software as a Service (SaaS)" delivers software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support.

   - Provides the consumer the ability to use the provider's applications running on a Cloud infrastructure.
   - The applications are accessible from various client devices such as a web browser (e.g., web-based e-mail).
   - 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.
   - Service provider manages and controls Cloud infrastructure (network, servers, operating systems) and makes its applications running on Cloud infrastructure available for access by customers

2) *Platform* -- Cloud Platform as a Service (PaaS)

   Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming Cloud infrastructure and sustaining Cloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.

   - Provides the consumer the ability 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.

- Service provider makes available technology infrastructure, including servers, network, operating systems or storage
- Customer maintains control over deployed applications and may control application hosting environment configurations

3) *Infrastructure* -- Cloud Infrastructure as a Service (IaaS)

Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients instead buy those resources as a fully outsourced service. Suppliers typically bill such services on a utility computing basis; the amount of resources consumed (and therefore the cost) will typically reflect the level of activity.

- Provides the consumer the ability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include 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).
- Provisioning of physical machines (e.g., server farms) at locations determined by provider, which are made available as a virtual machine to customer
- Customer retains control over, and responsibility for, deployed applications and storage, and may select networking components (e.g., firewalls and load balancers)

2.2 The Cloud v. Traditional IT Services Models

How do Cloud services compare with traditional IT services models, such as software licenses, traditional outsourcing?

a) Cloud v. software license

The Cloud is:

- installed on the provider's hardware, not on customer's
- accessed through Internet, not limited by customer's network
- use of software for prescribed functions only, with limited ability to customize/configure
- subscription pricing model based on usage metrics, not license + maintenance fee

b) Cloud v. outsourcing

With the Cloud:

- location of provider's server farm(s) unknown
- provider's hardware and network not dedicated to customer
- provider's employees not dedicated to customer
- subscription pricing model means no separate pricing for hardware maintenance, technology refresh or IMACs

2.3 Summary

The "economies of scale" of the Cloud allow for cost effective, flexible access to the latest quality IT resources at the quantity you need, when you need it.

Instead of owning and managing IT products and services, or using a "traditional" outsourcing approach built around dedicated hardware, software, and support services, organizations employing Cloud computing services can meet their ICT requirements

using a flexible, on-demand, and rapidly scalable model requiring neither ownership on their part, nor provision of dedicated resources by the Cloud services provider. Both parties stand to benefit from the considerable economies of scale and scope that are possible under such an arrangement.

The public sector, and municipalities in particular, are dominated by a “silo” model for IT services that sees many operating largely stand-alone information systems. The most significant Cloud computing opportunities for municipalities may arise as the Cloud serves as a catalyst for municipalities to share IT resources, whether on the public Cloud, or on a more localized Cloud deployment model.

While, in principle, Cloud computing is little different from more traditional outsourcing arrangements, municipalities should assure themselves that the security surrounding Cloud environments complies with laws, policies, and protocols.

3. WHAT ARE THE RISKS/CHALLENGES OF THE CLOUD

As with negotiating any contract for IT services, municipalities will want to be very careful to determine exactly what services are required, and exactly what services are being offered by the vendor, whether the two sufficiently match, and that all appropriate IT industry contract standards are covered.

Beyond the general challenges, the single most important challenge is that of privacy and security of information.

Security of information held in Cloud computing environments will be an area of significant concern for all levels of government.

3.1 Location of data and legal jurisdiction is a key unsolved question

The key challenge for a municipality is that, while a municipality can benefit from “outsourcing” IT services through the Cloud – a municipality cannot outsource responsibility for protecting the data.

Cloud computing is largely borderless as information in the Cloud typically frequently resides in different jurisdictions. Canadian laws will continue to apply to the activities, but so too will laws in other jurisdictions. Closely linked to issues of jurisdiction are those related to access to the data by foreign governments.

So the question is: How can a municipality outsource personal data for processing in countries with laws that allow arguably easier access (than those in Canada) on the part of governments to the data?

In many municipalities, the "head" of the municipality for the purposes of privacy legislation is the City Clerk, and the "head" bears responsibility for the protection of the data.[12]

Thus, even though the municipality may have a "Chief Information Officer" (CIO), it will likely be a separate City official (likely the City Clerk) who bears the statutory responsibility for the protection of the information. Therefore, the Clerk and the CIO should be working together (and should be working with an IT lawyer).

Given the release of direct control over information that Cloud computing entails, municipalities will need to thoroughly understand how privacy is assured in a Cloud environment. If information is held or processed in Cloud environments that are legally and/or physically located offshore, municipalities will need to clearly understand how

---

[12] For example: *Municipal Freedom of Information and Protection of Privacy Act*, R.R.O. 1990, REGULATION 823, GENERAL

> **3.** (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected. R.R.O. 1990, Reg. 823, s. 3 (1).
>
> (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it. R.R.O. 1990, Reg. 823, s. 3 (2).
>
> (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected. R.R.O. 1990, Reg. 823, s. 3 (3).

this may affect their ability to apply all relevant legal rights, restrictions, and sanctions that prevail in their own jurisdictions.

In some cases, they may find that the operation of various data protection laws[13] and protocols prohibits them from using some Cloud services. In this case, private Clouds may again offer an alternative solution.

Cloud computing that takes place solely in Canada may alleviate some of the concerns that are raised by data residing in or transiting other jurisdictions.

3.2 General Issues for consideration when contracting for Cloud services

a) SECURITY OF DATA

There are arguments suggesting that Cloud environments are more secure than many traditional enterprise IT systems. Whether the Cloud is more secure than your municipal client's IT system, or at least sufficiently secure, is a question for your client to consider, having regard for the following:

[13] Where is the data located?

- PIPEDA and provincial and municipal equivalents:

  Do users know that their data may be stored outside of Canada?

  Have they consented to this?

  Does the contract with the Cloud provider require the provider to protect the users' personal information?

- USA Patriot Act

  Risk of seizure by US government (or governments in other countries with similar laws)

Location of data, again:

Where the data is located is not only a privacy issue but is also a security issue. Think about the challenges one may face in preserving the integrity of government information held offshore and in having it repatriated, if required, in instances of natural disaster, political instability, civil or industrial unrest, criminal activity, terrorism, or any instance of *force majeure*?

This is not only a privacy law issue (think about the municipalities own financial data, or other strategic business documents/information). Again, this risk can be minimized through the creation of a private Cloud—particularly if that Cloud resides in the government's own jurisdiction.

Open system:

Aside from the location of the data, other security risks may lead to inadvertent disclosure of data where:

- data is sent over the Internet, exposing it to risks that are not present in a closed network
- data is stored on a shared resource – another user might gain access to it, intentionally or inadvertently
- large quantities of data are concentrated in one place – an attractive target for a malicious hacker or insider
- recovery from data complicated when data location or security controls cannot be tracked.

Multiple tenants:

A Cloud environment may have multiple tenants. A government may not know or trust all of these tenants, or wish to share computing resources with them.

b) CONTROL OF DATA

Where location of data is an issue for reasons discussed above, the most important question will be:

- Will the municipality be able to control the physical location of their own data?

Other important issues of control include:

- When data is “deleted” is it really gone?
- Can you provide access to an individual on request?
- Cloud providers may not be adequately prepared for disaster recovery. Clients should ensure proper test procedures are in place.
- What happens to data in the event of bankruptcy or acquisition of provider?
- Vendors may want a right to dispose of your data in the event of termination (such as for non-payment)
- Can organizations still comply with e-discovery/litigation hold requirements and policies?

c) COMPATIBILITY OF SYSTEMS

- Some Cloud computing networks may not be compatible with existing IT infrastructure.
- Over-reliance on a Cloud provider can lead to data lock-in.
- Cloud providers do not always warrant cross-compatibility with competing service providers.
- Risks of reliance on external systems can be mitigated through use of hybrid Clouds and contracting for transition services.

d) QUALITY OF SERVICE

- Factors to consider:
    - How critical is the service to the business?

    - What is the potential impact on the brand?
    - Does the service model meet all business requirements?

- Standard Cloud computing agreements:
    - contain no details regarding service levels
    - permit the provider to unilaterally suspend or terminate services
    - most providers will limit liability to a level that is not in line with potential risks
    - many allow for unilateral termination by provider upon little notice
    - disclaim: warranties, liability for poor service (or no service)

- Monitoring
    - Because all data is hosted off-site in multiple locations, monitoring service levels and data usage can be challenging.
    - Standard IT monitoring processes can be implemented by providers and should be requested by clients.
    - How can auditing rights be exercised?

- Standardization
    - Quality standards are still just emerging with respect to Cloud computing providers.
    - Standards mainly exist around technological aspects such as data formats, communication protocols and programming interfaces (i.e. .NET).
    - Few standards and benchmarks exist around configuration, management and maintenance of Cloud services. Simply importing “offline” standards into the Cloud environment may not always be practical.

e) PROCUREMENT

Another challenge may be the issue of procurement. Notwithstanding that many Cloud proponents (particularly in the U.S.) highlight ‘speed of procurement’ as a benefit to the

Cloud, Canadian municipalities are faced with a highly regulated procurement environment. Care will have to be taken to ensure that the relative ease with which municipal staff may in fact obtain Cloud services does not result in violations of the municipalities complicated procurement obligations as imposed under Canadian law.

The relative ease with which municipal staff may in fact obtain Cloud services also raises the question: to what extent is your municipal client already using the Cloud? Are some staff members in operational departments already using the Cloud to creatively provide IT solutions, without the knowledge of the CIO, the Clerk, purchasing staff or legal? To what extent does your municipal client already have some data on the Cloud that you don't know about?

3.3 Don't get lost in the Clouds! Practical Strategies to evaluate risks

The increasing buzz around Cloud computing has prompted municipalities to assess the Cloud as the newest IT delivery model. Although concerns, especially around privacy, security and sovereignty of data, do continue to inhibit adoption in many cases, the economic value of moving to the Cloud will continue to attract municipal interest.

Whether your municipal client is considering Cloud computing now or waiting until it becomes more mature, it is wise to monitor the development of Cloud computing and analyze how it might fit into the long term IT plans and strategies of your client.

- Understand your client:
    - current IT service capabilities
    - business road map and future needs
    - internal standards and restrictions

- Understand Cloud and other IT providers
    - What they can offer
    - History/length of reputation in the industry

In order to help your client to understand these issues, municipal lawyers, as trusted advisors to municipalities, can:

- encourage the municipality's Clerk and the Chief Information Officer (CIO) to work together, with a specialized IT lawyer;
- advocate on behalf the CIO/Clerk/IT lawyer team -- this is a core team that should be a part of any municipality's overall long range strategic planning exercise.

There are several steps that municipalities can take within the overall strategic planning exercise to ensure proper long range IT services that may include the Cloud:

- Identify data that cannot be held in public Cloud
- Develop a cost/benefit and risk evaluation framework to chart the decisions that will need to be made about where, when, and how potential Cloud services could be adopted
- Consider in-house infrastructure that may complement Cloud-based services in the future.
- Identify potential opportunities for switching from existing computing arrangements to Cloud services.

Cloud services are just one IT option. When making IT decisions, whether to opt for the Cloud or not, consider whether the decision is Cloud compatible for the future. For example, current infrastructure services decisions may support the ability of in-house IT to extend into some Clouds for additional compute and storage capacity of non-sensitive information.

Even if a Cloud based solution is acceptable now, remember that a shift toward some Cloud services is not an all-or-nothing decision. In each case, encourage your municipal clients to consult with legal on appropriate IT contract standards – and to know their exit route.