Wigley & Company

BARRISTERS and SOLICITORS

Cloud Computing for Public Sector Lawyers

16 June 2010

Public sector ICT will be revolutionised by cloud computing. Public Sector lawyers will increasingly be asked to advise on cloud computing raises. This paper provides an overview. More detail on public sector procurement is in our related article, *Public Sector procurement and cloud computing*. There are two other related articles: (a) *Cloud Computing the reality; government procurement; and regulationanti-trust Address at Communicasia Singapore* (b) *Cloud Computing: Regulatory/Anti-trust risks and solutions.*

Table of Contents

Introduction

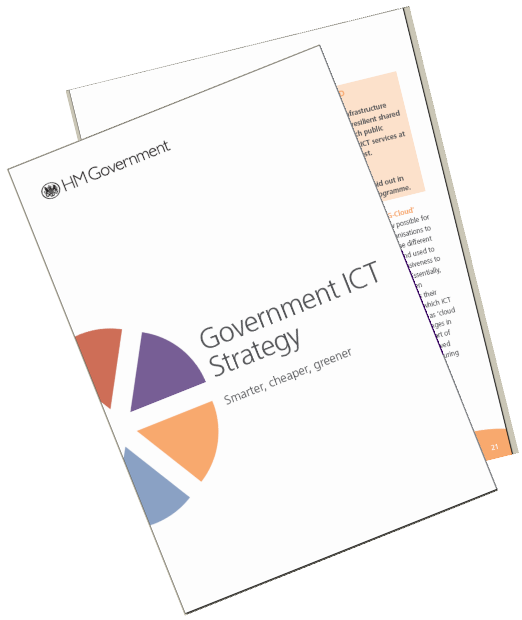
In this paper, we overview what cloud computing is, why government is doing it, and the issues for lawyers.

> *"The Government Cloud Infrastructure will provide a secure and resilient shared environment through which public sector bodies can resource ICT services at greater speed and lower cost."* [1]

These services are available at infrastructure, services and platform levels. Typically, an agency, at least initially, will have a combination of legacy solutions (e.g. based on servers and dedicated software on the agency's premises) and cloud solutions (solutions provided from elsewhere, whether inside or outside the Government's own "cloud").

For lawyers advising the public sector, this raises a number of issues. Key issues are summarised below, with reference to other papers we have written.

For example, whether the agency can transition from current legacy contracts or re-negotiate them is likely to be a key issue on which good legal and strategic advice will



provide wins: it will be possible to do this more

[1] *UK Government, Government ICT Strategy - Smarter, cheaper, greener*, January 2010.

than appears at first sight. This important issue is covered in our related paper on *Public Sector Procurement and Cloud Computing*.

Other key issues include privacy and security, quality of service commitments and service level agreements, etc.

What is cloud computing?

Well known examples of cloud computing are the Xero accounting package (this type of service is also called Software as a Service or SaaS), Hotmail, Facebook, and Amazon's and Google's cloud services.

Many things are encompassed in "cloud computing" and much time is wasted figuring out definitions.

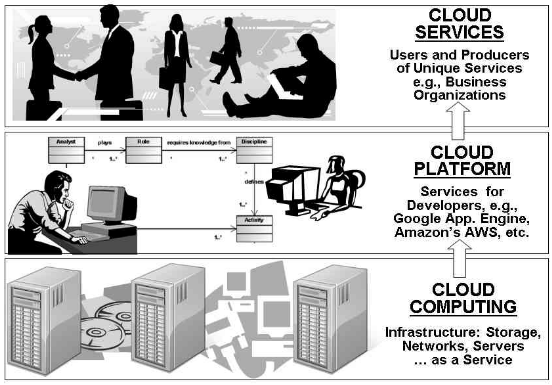
A simple definition in a government context is:[2]

> The term "cloud computing" refers to the delivery of ICT resources over the internet rather than hosting and operating these resources locally on an individual department's network. The concept can be compared to changes in the electricity industry during the early part of the 20th century as organisations moved from buying their own generators to procuring electricity as a utility.

Cloud computing crops up in many ways. For example, it may be about sharing infrastructure. In a government context, it may be decided that the data handled by government is so sensitive, and the need for strong quality of service so high, that it is best to keep the cloud infrastructure within government servers, etc.

[2] From the UK Cabinet Office website, another of many definitions is:

Cloud computing is a style of computing in which dynamically scalable and often virtualised resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. … Cloud computing services often provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers.



Maybe, as in the UK, a handful of data centres will be established for use by all of the public sector, to replace the numerous data centres used by public sector agencies. That would happen instead of allowing hosting and processing of data offshore and by third parties.

Much public sector data could easily be handled off shore. Public sector agencies have judgment calls to make.

New Zealand Post

For example, New Zealand Post uses Google applications (a type of cloud computing solution). However, it minimises risk by requiring Google to keep the data within Australasia (e.g. it can't go to Europe, Asia, etc).

Why will the public sector move toward cloud computing?

At a high level, reasons include:

- Significant cost savings (for some countries this may be as much as a 20% reduction in ICT spend, so the drivers are strong).
- Reduced energy consumption.
- Greater public sector business flexibility (rather than be tied to legacy services on an agency's own equipment and software with associated cost and vendor lock-in), shared common infrastructure can be used, and capacity sourced on an "on demand' basis.

In more detail, the UK Government CIO sees the strategy as:[3]

1. Standardise and simplify the desktop.
2. Standardise, rationalise and simplify the plethora of networks.
3. Rationalise the data centre estate.
4. Deliver against the Open source, open standards and reuse strategy.
5. Green IT.
6. Information Security and Assurance.
7. Shared Services.
8. Reliable Project Delivery.
9. Supplier Management.
10. Professionalising IT Enabled business change.

UK Example

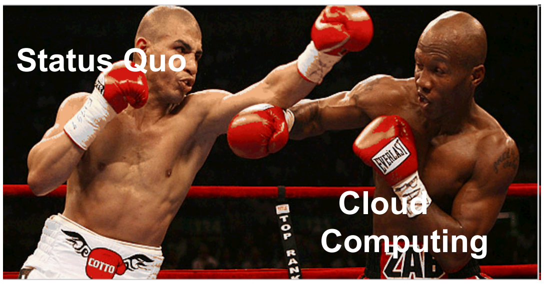
- In the UK, it's said:[4]

> The "G-Cloud" strategy came with claims that it could save government £3.2bn of its annual £16bn IT budget – perfectly meeting the chancellor's 20% savings target. The proposal is to replace the current ad-hoc network of department-hosted systems with a dozen dedicated government secure data centres, costing £250m each.
>
> The G-Cloud plans could support everything from pooled government data centres to a communal email solution, collaboration tools and staff-editable wikis (like Wikipedia, but private). Part of the plan points to the potential of an internal government "app store" so that recommended tools could be shared and distributed among government departments. By 2015, the strategy says, as much as 80% of the government departments could be using this system.

When assessing risk, compare the status quo with cloud computing

We deal in more detail with this in our paper, *Cloud Computing: the reality; government procurement;* and *our address at Communicasia Singapore*.

There is a tendency to compare cloud computing with perfection. But the comparison is with the status quo. Often, the human security issues in an office environment and ICT systems will be much higher than the security issues around cloud computing.



Example: Security

Security and privacy are important topics but must be put in context. We deal with this our article, *Cloud computing: privacy and security issues*.

It is worth repeating the point made in our *Cloud Computing: Public Sector Procurement* paper in relation to security. Contrary to the perceived greater security risk in the cloud, the UK Guardian reported:[5]

> Kate Craig-Wood, co-founder and managing director of cloud hosting firm Memset, based in Guildford, has been heavily involved in the development of the G-Cloud strategy...Craig-Wood insists a move to the cloud would mean improved security, because individuals couldn't download a large volume of data to CD – and then leave it on a train. Services would be classified – and then clustered – according to "impact levels", so low-security projects such as government information sites could be hosted on public clouds, and confidential data hosted in a private, secure

[3] http://johnsuffolk.typepad.com/john-suffolk---government-cio/cloud-g-cloud/.

[4] Quoted from the Guardian (June 2010) at: http://www.guardian.co.uk/cloud-computing/g-cloud-would-help-the-government-to-save.

[5] http://www.guardian.co.uk/cloud-computing/g-cloud-would-help-the-government-to-save.

> government cloud. (Under the plans the security services would remain separate from the G-Cloud).

This doesn't mean that security and privacy are always safer in the cloud. That will depend on circumstances, which countries the data goes to, applicable legislation, and so on.

Key issues for lawyers reviewing cloud computing contracts and overall risks

This is not a comprehensive list, and some issues are covered in the related papers noted above (for example, major procurement issues as to cloud computing are covered in the related paper, *Public Sector procurement and cloud computing*).

Issues will differ according to circumstances and whether the data goes off-shore or remains in the country (perhaps only on government infrastructure and systems). These issues include the following:

- Legislative and governmental issues such as the Privacy Act, the Public US Records Act and offshore legislation such as the Patriot Act (US). Also sovereignty issues. See above.

- SLAs: so far, the quality of service level agreements provided by cloud computing providers tend to be lean. These are likely to improve over time as services mature, and the demand from large organisations increase.

- Quality of Service; Related to SLAs, this involves considerations such as the reliability of the service, etc.

- Ability to transition out. This is a key issue. The ability to take data away from the provider to another and have it processed, etc, with relative ease. As above, the comparison is with the status quo. Customers can find it difficult to transition from legacy systems.

- A related issue: can the provider delete the customer's data. Some providers' contracts allow them to do this. This issue relates to disaster recovery and backups as noted below.

- Inter-operability: see our paper, *Regulatory/Anti-trust risks and solutions*.

- Security/Privacy/Confidential information (see above and also the government security guidance (e.g. Security in Government (SIGS) in NZ).

- International issues. (See above).

- Disaster recovery/Backups, etc. This is an important issue. Who handles DR and backups: the customer and/or the supplier? Or maybe a third party as well or instead.

- Regulatory. See the related article, *Regulatory/Anti-trust risks and solutions*.

We also recommend, where data will be transferred offshore, the SSC comprehensive guidance in *Government Use of Offshore Information and Communication Technologies (ICT) Service Provider-Advice on Risk Management.*

Those guidelines note at page 38:

> Some topics to discuss with your legal advisors: When contemplating contracting for services with an offshore supplier, agencies may wish to discuss the following issues with their legal advisors. The list below is not intended to be exhaustive and the importance and negotiability of such issues is likely to depend on the magnitude of risk and value of the contract.
>
> - Procurement implications.
>
> - Ensuring the contract deals appropriately with ownership and licensing of intellectual and other property, including personal information and other data and, where relevant, derivative works.
>
> - The potential desirability of obliging the service provider to advise the New Zealand agency of any relevant changes in legislation, regulations and other controls on operations that are imposed on the provider

by its home or operating jurisdiction.

- The potential need for clear definitions of terms, processes and behaviours that are significant to the operation of the contract and which, in the absence of clear definition, may be interpreted differently in the other jurisdiction.

- Prescribing contractual processes for handling project risks and issues and matters of change control.

- The potential need for provisions dealing clearly with matters of reporting, governance, audit, acceptance testing and liability.

- Considering the choice of law and forum for disputes, and the practical implications of these.

- The need for clear and appropriate escalation paths and dispute resolution processes.

- The potential need for change of ownership/control provisions.

- Where personal information is at stake, the desirability of data breach notification mechanisms.

- In significant projects, the potential need for a performance bond or guarantee.

- The potential application of, and compliance with, the *New Zealand Government Web Standards and Recommendations and Web Site Outsourcing Guidelines*.

- The potential desirability of including a prohibition on sub-contracting without the agency's express written consent.

- The advisability of carrying out a check on the financial health of the company with which they are planning to do business.

We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.

Wigley & Company is a long established specialist law firm. Our focus includes IT, telecommunications, regulatory and competition law, procurement and media/marketing. With broad experience acting for suppliers and customers, government agencies and corporates, Wigley & Company understands the issues on "both sides of the fence", and helps clients achieve win-win outcomes.

With a strong combination of commercial, legal, technical and strategic skills, Wigley & Company provides genuinely innovative and pragmatic solutions.

Wigley & Company, Barristers & Solicitors | E: info@wigleylaw.com | P: +64 (4) 472 3023