Solicitors Regulation Authority

# Silver Linings:

## cloud computing, law firms and risk

November 2013

# Contents

# Executive summary

The Risk Outlook 2013 highlighted 'lack of due diligence over outsourcing arrangements' as a potential risk. Whenever firms outsource activities, it is important that appropriate controls are in place to manage associated risks.

Cloud computing involves outsourcing data processing and storage to an external provider. The risk of firms failing to exercise due diligence in controlling the risks of such outsourcing systems was included as a potential risk in our 2013 Risk Outlook.

Public cloud systems involve the user surrendering true control of their data and software to a remote provider. Data is pooled, and confidentiality is protected by encryption and password log-ins rather than by physical separation.

Private cloud systems retain separate areas for individual users' data. This increases control at the expense of cost.

Hybrid cloud systems permit the use of both private and public areas for data, usually with public cloud storage used flexibly to supplement a private system.

Cloud computing is continuing to increase in popularity, with low cost and flexibility the key advantages. Cloud users do not have to maintain their own data storage or multiple site licenses for software. The cloud works out cheaper than direct data and program storage, and permits true mobile working with no need for data sticks or email transmission of files, both of which are key risks for data loss. Email is not inherently secure, while data sticks are easily lost and provide ready systems access for virus programs.

Firms are obliged to keep client information confidential. This does not bar them from using cloud systems, but they do have to ensure that the system that they choose provides sufficient protection.

Sound cloud computing providers offer better encryption and security than would be possible for a small or medium-sized solicitors' practice storing its data locally.

Firms must be able to ensure that their provider can agree to SRA access to inspect data in order to meet Outcome 7.10 of the SRA Code of Conduct.

Use of cloud systems makes server downtime a business-critical issue. Firms must ensure that providers offer appropriate guarantees and that data is protected in the event of technical failures or the provider becoming insolvent.

Use of cloud systems must comply with the terms of the Data Protection Act 1998. These terms require a written contract between user and provider and restrict the sending of data out of the European Economic Area ("EEA"). Potential users must familiarise themselves with the requirements of the Eighth Principle to the Act before committing to a provider.

Due to the heightened requirements of client confidentiality faced by law firms, they should conduct due diligence on any proposed provider to ensure that it can meet the requirements of a legal business before they make a final commitment. Given the nature of US surveillance laws, law firms should take into account how they use US-based providers or providers that use US servers.

Best practice for due diligence includes:

- taking references from other companies using the proposed provider
- checking service level agreements carefully to ensure that the proposed service can offer at least full Safe Harbour compliance if data is stored outside the EEA
- checking that the provider can offer audited information security that at a minimum is compliant with ISO27001 2005
- checking that the provider can offer a level of guaranteed uptime and continuity protection that is acceptable to the firm
- ensuring, where staff will be working on the move, that they have properly secured communication channels to protect security
- ensuring that their contract with the provider includes the requirements of Outcome 7.10 of the SRA Code of Conduct.

Security can also be improved by:

- using a private cloud, or private area of a hybrid cloud, for client confidential material
- using software to automatically encrypt documents at the law firm's end, using security keys that are not known to the provider
- using only providers that are based in EEA countries or countries offering equivalent or greater data protection laws, and that can guarantee that data will not be held in jurisdictions that do not offer such protections

# Background

This document provides a brief overview of cloud computing and sets out the SRA's view of the risks posed by its use by law firms.

This form of provision involves data and software being held, not on the user's own server, but on remote servers operated by a separate provider. The user simply logs into the service and accesses both programs and data remotely, with an experience that ideally should be indistinguishable from that of using a traditional system[1].

As with any form of outsourcing, it is important that firms using cloud computing exercise due diligence in controlling the risks. Our 2013 Risk Outlook listed the risk of firms failing to exercise such due diligence as a potential risk. With the use of cloud computing increasing, this remains the case.

Take-up of these remote delivery applications is spreading rapidly. To take an example from one major provider of remote systems to business, Citrix claims that its current delivery system, XenApp5, is in use by over 100 million users worldwide.[2] More than 30 percent of enterprises worldwide, and many individuals, now use some form of cloud provision, a proportion which is expected to increase dramatically[3].

Cloud computing comes in three forms: Public, Private and Hybrid.

## Public clouds:

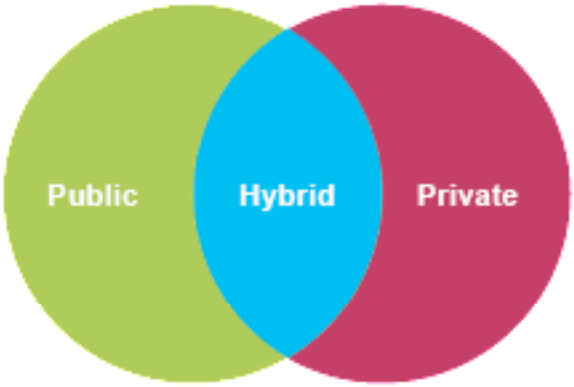
- store data in a network of computers, with server use pooled among a number of clients
- providers often subcontract server capacity for reasons of flexibility, so may not be able to tell where any particular client's data is held
- this is the most flexible, and cheapest, form of provision

## Private clouds:

- store data using resources dedicated to the client
- this may mean using the client's own servers with a cloud technology for access, or may mean dedicated server space at the cloud provider's data centres
- this provides greater security and control for the client, but at significantly greater cost

## Hybrid clouds:

- combine aspects of both public and private clouds, often involving private cloud storage that is supplemented by public cloud use on an as-needed basis.




In all cases, the user will have a service level agreement with the provider defining the terms on which data is to be processed.

1. Morin, M, "What is Cloud Computing? Interviewing Dave Vandervort of Xerox Innovation Group", Ruby About.com. http://ruby.about.com/od/cloudcomputing/a/dvandervort.htm.
2. Citrix XenApp guidance. http://www.1st-computer-networks.co.uk/citrix_xen_app.php
3. Van der Zwet, J (2012), "Layers of Latency: Cloud Complexity and Performance", Wired, 18 September 2012. http://www.wired.

# Reasons why firms use cloud technologies

## Lower cost of provision especially of specific software

Public cloud computing in particular is much cheaper than traditional IT provision. It has been estimated that users of public cloud computing systems can see up front savings of 40-to-50 percent[4]. Costs can also be flexible. Firms can pay for the software they use as they use it, without minimum pricing or any necessary long-term commitments.[5]

The same feature makes it simple for firms to upgrade their software and to introduce new types of machine, such as tablets for mobile working.

As processing power can be supplied centrally, users can obtain more advanced and effective systems that they would otherwise be able to run on their own network and machines. The economies of scale offered by large cloud providers also let them provide more potent systems at a lower cost, with a 5-to-10 percent efficiency saving on the pricing of systems.[6]

The possibility of having software and data centralised on an accessible remote platform also allows for bring-your-own-technology policies, which some businesses have found to both motivate staff and reduce costs.

## Mobile access

The fundamental point of cloud computing is that it does not matter what machine the user is working from. As long as they have their log-in details, then they should be able to access the same data and software wherever they are. This is an enabling technology for true mobile working, with fee earners able to access key documents anywhere.[7] Even firms that do not intend to use mobile working, but which do need a certain amount of hot-desking, should see benefits from non machine-specific access to data.

## Maintenance

Cloud systems make it possible to have maintenance of IT systems conducted entirely remotely, by the provider. Maintaining local servers requires a local IT support staff, whether working for the firm or outsourced, to ensure that the systems remain operational. By contrast, with a cloud system, the servers are all the responsibility of the provider. This lack of any need to maintain an IT support department has explicitly been cited by one law firm as a reason for adopting a cloud provision model.

## Access to technology

The flexibility, cost and ease of maintenance offered by cloud computing systems make them simple for less experienced and well funded firms to use. These systems may enable small law firms to gain the benefits of information systems that they could not otherwise access at all.

---

4. Tisnovsky, R (2010), “Risks Versus Value in Outsourced Cloud Computing”, Financial Executive 1 November 2010. Citrix also claim a 50% saving on up-front costs for implementation of XenApp: Citrix XenApp Guidance. http://business.highbeam.com/388/article-1G1-243279222/risks-versus-value-outsourced-cloud-computing

5. Tisnovsky, R. http://business.highbeam.com/388/article-1G1-243279222/risks-versus-value-outsourced-cloud-computing

6. ibid. http://business.highbeam.com/388/article-1G1-243279222/risks-versus-value-outsourced-cloud-computing

7. As with Eversheds' programme: Barrington, M. “Eversheds Announces Pilot iPad Programme For its Lawyers”. http://ipadlawyer.co.uk/eversheds-announces-pilot-ipad-programme-for

# Compliance and legal issues with cloud computing

When considering adopting a cloud computing system for their business, firms must take into account the regulatory and legal rules which apply.

In regulatory terms, outcome 7.3 of the SRA Code of Conduct requires firms to identify, monitor and manage risks to compliance and take steps to address issues identified. Firms should consider carefully what risks the use of the chosen system poses to them and clients and take steps to address these.

The principal legislation that firms must take into account is the Data Protection Act, 1998.

The regulatory and legal issues are summarised below.

## SRA Code of Conduct

### Dealing with the SRA

Principle 7 of the SRA Handbook requires solicitors to comply with their legal and regulatory obligations and deal with their regulator in an open, timely and co-operative manner. Firms will in part be complying with the principle by achieving outcome 7.10 of the SRA Code of Conduct, the purpose of which is to ensure that they have appropriate terms in their agreement with the provider, allowing the SRA to access the information stored.

There may be practical difficulties in accessing the information if it is stored overseas, but the point of the outcome is to try to reduce the risk of such difficulties. As with all of the outcomes, whilst firms must achieve them, the manner in which they do so is for them to determine. However, firms should bear in mind the potential risk in respect of costs as well as under Principle 7. It would be sensible for the agreement to include a term requiring the provider to deliver data, in a usable form, to the SRA on demand. To be effective, such a term must make the requirement binding notwithstanding any dispute between the firm and the provider or any breach of the agreement on the part of the firm.

### Confidentiality

Outcome 4.1 requires solicitors to keep the affairs of clients confidential. This does not prevent firms outsourcing services. Indicative behaviour 4.3 is one way of evidencing compliance with the outcome, involving satisfaction that the provider has taken all appropriate steps to ensure that clients' confidential information will be protected. Firms should consider carefully the provider's systems for protecting confidentiality. To protect themselves, they should check whether, in addition to a confidentiality term, the agreement sets out specifically what the security measures for the data centres must be.

Firms should also consider the locations of the data centres and whether local laws could pose a risk to confidentiality by requiring the provider to disclose confidential information. In any event, it is advisable to require in the agreement that the provider notifies firms of any such request they receive, as well as any breach of their security arrangements. As the same legislation may prevent providers in certain countries from meeting this requirement, firms relying on this provision will need to take into account whether their proposed provider can meet it.

Bearing in mind the requirement under outcome 7.3 to monitor risks, firms will need to consider what checks they should undertake, and how often, to satisfy themselves that the provider is complying with the agreement. It would also be advisable for the agreement to require the provider to undertake an annual audit of its security measures.

The need for these requirements in a service agreement with a cloud provider is one reason why free public cloud services will not generally be suitable for confidential client information.

### Loss of data control

To minimise the risk of being in breach of Principles 4 and 5, it is advisable to ensure that firms have the right to get data back in a usable format on demand and that they retain full ownership of the information stored. Firms should also ensure that they are aware of, and satisfied with, the arrangements under the agreement for:

- frequency of back up of data
- continuity and portability of the data in the event that the provider's business fails (for instance through insolvency) or you wish to switch to another provider

Escrow systems may in some circumstances be available to ensure continuity and control.

### Availability of the system

Service interruptions and downtime may potentially put firms at risk under Principle 5 of the SRA Handbook and Outcome 1.2 which requires them to provide services to clients in a manner which protects their interests in their matter. The service level agreement with the provider is likely to specify the uptime, but firms should check the definition of 'up' and ensure they are satisfied with the guarantee provided. As part of basic due diligence, it is advisable to take up references, as well as asking for evidence of the provider's history of downtime and the steps they have taken to prevent future problems.

Bearing in mind the risk which downtime will pose to business, firms would be advised to check that the agreement clearly states what redress will be available in these circumstances and consider carefully whether this is sufficient in view of the potential impact of a serious outage.

### Client care

From a client care point of view, firms need to bear in mind outcome 1.12, which requires clients to be in a position to make informed decisions about the services they need, how their matter will be handled and the options available to them, and outcome 4.2, which requires the fee earner to disclose to the client all information which is material to the client's retainer of which the fee earner is aware. Solicitors have implied consent to confidential information being passed to external IT service providers. Given the potential risks of cloud computing, it would, however, be prudent to inform clients in your terms of business that the firm uses cloud computing. However, there may be circumstances where this would not be sufficient and informed consent would be advisable. Firms should consider their clients individual needs and whether, in certain matters, the risk to confidentiality is too great. Where the matter is an unusually sensitive or high profile one, firms are advised to discuss with the client and get informed consent to any sharing or passing of client information.

### Data Protection Act

As with all other firms, solicitors must comply with the Data Protection Act 1998 (DPA) in handling personal data. It is not a breach of the DPA to transmit data to an outsourced IT provider. Under the Personal Information Online Code of Practice, however, if personal data is to be stored on a cloud, then there must be a written contract in place requiring the provider to act only on the user's instructions. The provider must have a level of security which meets the information security provisions of the seventh principle of the DPA.

It is important to be aware of the eighth principle of the DPA. This states that personal data may not be transferred outside the European Economic Area unless the country to which the data is transferred ensures an adequate degree of protection. The European Commission recognises a list of non-EEA countries which are deemed to meet this requirement, and maintains "Safe Harbour" agreements which US-based companies can sign up to (see appendix).

The implication of this is that the firm must know whether their data is to be stored outside the EEA.

Users will need to check terms of service carefully and may need to specifically agree necessary guarantees before contracting for provision.

The application of the DPA to online systems is detailed in the Information Commissioner's Office's Personal Information Online Code of Practice[8]. This code contains specific guidance for the use of cloud computing systems.

The code notes that firms using cloud computing may not know where their information is being processed, and that due to chains of subcontractors they may not even know who is processing the information on their behalf. As such, the code notes that organisations must not relinquish control of personal data or expose it to risks which would not have been incurred had the data been processed in the UK. There must be a written contract in place with the provider, which can be electronic, requiring the provider to follow the user's instructions and have an equivalent level of security.

The code further regards it as being good practice to encrypt data prior to transferring it to the online services company, providing an additional level of protection regardless of the jurisdiction in which the data is held.

This is a necessarily brief summary of the DPA requirements for cloud computing. Firms considering adopting cloud systems should familiarise themselves with the full code of Practice.

8. Graham, I (2010), "Personal Information Online Code of Practice", Information Commissioner's Office July 2010. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf

# Risks for law firms from cloud computing

The use of cloud computing involves risks to the regulatory objectives in the Legal Services Act 2007. It can, however, also help to control risks. Firms should consider their own circumstances and needs carefully when deciding on adopting these systems.

## Breach of Confidentiality

### Positives

The use of cloud computing can improve general data security. Data service providers will usually have more experience in protecting data than their clients will, and have access to stronger security and encryption.

The biggest data risk comes from lost or stolen laptops and USB drives. Google estimate that one in ten laptops go missing in the first year of use, and state that two thirds of workers report having lost a USB drive.[9] Cloud systems remove the need for USB drives and mean that data need not be kept on individual laptops.

Use of cloud computing systems may also help in reducing the risk of data theft by employees. A 2009 survey suggested that one in three Wall Street and Canary Wharf workers had made unauthorised use of their employer's data.[10] With audit trails and fewer untraceable means of storing confidential data, data theft is harder.

USB drives can also be a key vector for the transmission of Trojan Horse programs and viruses[11]. Eliminating any need for them improves data security. Similarly, removing the need to transmit working files by email removes an insecure means of data transmission.

With data stored remotely on the cloud and with computers properly configured to require log-ins and passwords before connecting to the provider, information will not be leaked in the event of a burglary at the firm's offices.

### Negatives

#### Issues with transferring data control to a third party

Cloud computing, by transferring control of data to a third party, shifts the task of preventing data leaks largely to the provider. Responsibility for preventing those leaks remains with the user.

Whilst good cloud providers will maintain very strong encryption and data security systems, less effective providers may not. It is important that law firms considering using a cloud computing system check that their prospective provider can be relied upon. The main information security standard is ISO 27001 2005: providers information security should be to at least an equqivalent standard.[12] Given the importance of legal privilege and client confidentiality, law firms should exclusively use established, known and well-regarded cloud providers.

At the users' end, normal confidentiality precautions such as regularly changing passwords and not writing passwords down remain critical.

---

9. ibid. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf

10. "Over a Third of Wall Street and Canary Wharf Workers are Stealing Sensitive Data", Computer Weekly 23 November 2009. http://www.computerweekly.com/news/1280091445/Over-a-third-of-Wall-Street-and-Canary-Wharf-workers-are-stealing-sensitive-data

11. See e.g. Rash, K (2011), "Stuxnet Turns USB Memory Sticks into Weapons of Mass Destruction", Eweek 16 February 2011. http://www.eweek.com/c/a/Security/Stuxnet-Turns-USB-Memory-Sticks-into-Weapons-of-Mass-Destruction-334848/

12. ISO (2007), "An Introduction to ISO 27001", International Standards Organisation 2007. http://www.27000.org/iso-27001.htm

Users will also need to ensure that they comply with the requirements of the provider in establishing and maintaining secured channels between their and the provider's systems. No cloud provider's system can protect the user from data loss at the user's end, for instance from the use of unsecured wi-fi.

Although rare, there have been cases of data loss from cloud providers. Firms should consider carefully the consequences should large numbers of client files end up being leaked, whether by data intrusion from outside or by a rogue employee, into the hands of identity fraudsters or of a group such as Wikileaks.

One significant recommendation from the IT field to help prevent risks arising from data loss from the provider is that users encrypt their own critical files before storing them on the cloud. Such encryption ensures that any leaked information from the provider cannot be read by third parties or, importantly, by corrupted staff at the provider.[13] Systems exist to perform this task automatically.

Another protection is to ensure that client confidential material is kept on a private cloud, with less sensitive information on public cloud.

### Issues with mobile working

Cloud computing makes mobile working easier. This creates the risk of confidentiality breaches as a result of eavesdropping, particularly where lawyers need to access their systems on the move. Public wi-fi is not guaranteed to be secure and can be subverted. The remedy for this is the establishment of a secure communications channel to eliminate electronic eavesdropping. This is a standard and widely used technique and one that all businesses using mobile working should be employing.

### Issues with sending data out of the country

Under principle 8 of the Data Protection Act, personal data may not be transferred out of the EEA unless the territory to which it is sent ensures an adequate level of protection — and the list of countries which have had findings of adequacy is limited. The list at the time of writing is given in the Appendix. Users need to be able to show that the data is stored in a jurisdiction subject to a finding of adequacy, or use a US provider that has "Safe Harbour" status. The difficulty is that, in a public cloud, there may be no way even for the provider to know specifically where any particular item of data is stored. As such, it may not be possible for some public cloud providers to comply with the requirements.

13. Binning, D (2009), "Top Five Cloud Computing Security Issues", Computer Weekly 24 April 2009. http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm

## The USA

The USA requires separate mention for two reasons:

1. The high concentration of technology companies, including cloud providers, that are based in that country; and:

2. Weak US protections for personal data, coupled with strong data seizure powers and intrusive surveillance.

Recent news coverage of US National Security Agency activities conducted under the terms of the PATRIOT Act[14], including acquiring data from providers such as Google under the PRISM programme, has brought this issue to public attention.

The exact details of the NSA programmes remain unclear at the time of writing, but it does appear that the US government has the ability to examine "metadata"–information such as the recipients and subject lines of e-mails–at will, and can more selectively obtain the content of information directly from providers.

The harvesting of metadata reveals networks of individuals. This may represent a confidentiality issue, for instance when firms are acting in confidential merger negotiations.

Information held by governmental agencies can leak, as shown by the PRISM publicity. There have been allegations, denied by such agencies[15], that information gathered by these means has in the past been passed to commercial organisations for business advantage. With the heightened need for confidentiality of law firms, this represents a challenge to their ability to use cloud services.

Given the risk to confidentiality from data seizure and surveillance policies, law firms should give serious consideration to the risks of storing data in countries with weak data privacy protections.

If firms do intend to use US providers, then they must at a minimum ensure that the provider can meet the terms of Safe Harbour.

Given the possibility of data seizure from the provider, the recommendation to encrypt sensitive information at the user's end is of particular importance in this case.

14. Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism ("USA PATRIOT") Act 2001 (USA). http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

15. See e.g. Asser, M (2000), "Echelon: Big Brother Without a Cause?", BBC 6 July 2000. http://news.bbc.co.uk/1/hi/world/europe/820758.stm

## Failure to Co-operate or Comply with Notification and Information Requirements

### Negatives

Firms dealing with cloud providers must be able to meet the requirements of Outcome 7.10 of the SRA Code of Conduct, which requires contractual terms authorising the SRA to access data and visit provider premises.

Compliance with this may restrict the range of possible providers. Changes in provider policies may affect their ability to comply.

At all times, firms must ensure that their cloud computing arrangements remain compliant.

## Structural Instability

### Positives

The intelligent use of cloud systems can reduce the risk of data or continuity loss. Most of the large cloud providers' service level agreements offer very high levels of uptime[16] and the use of multiple backup servers and sites by such companies means that the risk of irrecoverable data loss is very low[17]. Servers in a firm's own office, by contrast, can be lost in a fire or burglary.

### Negatives

**Server downtime**

The use of a cloud system means that all a firm's IT and data is supplied virtually from the provider. This makes server downtime a significant risk. It has been estimated that downtime can cause business losses of up to £10,000 per hour and up to £1 million if a full business day is lost.[18]

Cloud providers need to get the maximum use out of their systems to boost revenue. This gives an incentive to overload their system, and can lead to downtime. Cases of service interruptions lasting up to 22 hours have occurred.[19] Should a provider suffer significant technical failure or be caught up in an electronic attack on themselves or on one of their clients, as happened to the EveryDNS domain name provider in December 2010[20], then there may be the potential for greater downtime.

Firms adopting cloud provision should carefully examine the service level agreement that they are signing up to, in order to determine whether it guarantees 24 hour availability. They may also wish to check that redress is provided for in the event of loss due to downtime. Large and well established providers will have greater resources and better organisation to prevent significant downtime risks.

**Provider failure**

Any business can fail. This creates the possibility for serious data loss if a cloud provider goes bankrupt. Users need to establish that their provider has proper continuity arrangements to protect data in the event of provider failure[21]. As ever, the use of established and reputable providers provides good protection against this risk.

16. "Verio and Citrix to Power New Cloud Service Offering", DABCC 11 April 2012. http://www.dabcc.com/article.aspx?id=19881
17. Moazzezi, O (2012), "How Secure is the Cloud?", Computer Technology Review 5 March 2012. http://wwpi.com/index.php?option=com_content&view=article&id=14353:how-secure-is-the-cloud&catid=322:ctr-exclusives&Itemid=2701741
18. "Don't Get Trampled in the Stampede to Adopt Cloud Computing", National Computing Centre 2012. http://www.ncc.co.uk/article/?articleid=16092
19. Tisnovsky, R (2010), "Risks Versus Value in Outsourced Cloud Computing", Financial Executive 1 November 2010. http://business.highbeam.com/388/article-1G1-243279222/risks-versus-value-outsourced-cloud-computing
20. Tey, L, "Cloud Customers Risk Collateral DDOS", SC Secure Business Intelligence 24 February 2011. http://www.securecomputing.net.au/News/249231,cloud-customers-risk-collateral-ddos.aspx
21. Brodkin, J (2008), "Gartner: Seven Cloud Computing Security Risks", InfoWorld 2 July 2008 http://www.infoworld.com/d/security-

# Conclusion

Firms are increasingly using software as a service and cloud computing to deliver their IT needs. The reasons for this are price, flexibility and a desire for mobile working independent of specific machines. The high security and backup facilities made possible by the larger cloud providers are also desirable features.

Law firms whose use of cloud computing has been publicised have used it for purposes ranging from a cheaper and more flexible means of delivering traditional structures through to using it as an enabling technology for a fully virtual model.

We seek to encourage the development of an efficient legal services market, and regulate based on risk. The Solicitors Regulation Authority recognises the benefits of advanced information technology architectures. It is, however, our role to consider the risks arising from such new technologies.

The major threat from IT systems is that of a confidentiality breach. One of the major advantages of a cloud system is that it enables mobile working without the need to carry data around on laptops or datasticks, which are the main risks for data loss. Passing data to a remote provider does, however, create risks from the activities of staff who are not under the firm's control.

Governmental data seizure and surveillance powers represent a significant challenge to law firm use of cloud systems, in particular those based in countries with weaker data protections than those in the EEA.

The SRA recognises that provided an effective provider is used, cloud computing can provide benefits for the firm and for clients, both in terms of costs and providing better levels of encryption and security, and the SRA Code of Conduct ('the Code') does not prevent you from entering into such an arrangement. However, there are obvious risks, one of which is giving up control of your data to a third party which has the potential to compromise the SRA's ability to properly regulate the affairs of a firm and ensure that the interests of clients remain fully protected (for example, if a firm becomes insolvent, or subject to an investigation or intervention).

The risks of cloud computing are relevant to many other forms of outsourcing. Firms must evaluate their exposure to risks in accordance with their own tolerances and operating needs.

# Appendix: Findings of Adequacy

The Data Protection Act requires that "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

Firms outsourcing data processing to providers within the EEA therefore face no restrictions in sending personal data to those providers.

The European Commission maintains a short list of countries that it considers to have "adequate" levels of protection. These countries, at the time of writing, are:

- Andorra
- Argentina
- Canada
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay[22]

The USA has not received a Finding of Adequacy. The European Commission accepts that personal data sent to US companies is adequately protected if those companies have signed up to the voluntary Safe Harbour Agreement. Firms seeking to use US providers must ensure that their prospective provider has signed up.

It is permissible to send data to a country that is not on the list under certain circumstances beyond the scope of this paper. Firms seeking to investigate this possibility should refer to the Information Commissioner's Office.

22. "Sending Personal Data Outside The European Economic Area", Information Commissioner's Office. http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_8

# Index of Sources


"BPOS: a Data Leak in Microsoft's Cloud", *GNT* 28 December 2010. Online at: http://us.generation-nt.com/cloud-computing-data-leak-bpos-microsoft-news-2656841.html

"Don't Get Trampled in the Stampede to Adopt Cloud Computing", *National Computing Centre* 2012. Online at: http://www.ncc.co.uk/article/?articleid=16092

"Google and Data Protection Act and FSA Regulations", *Cloud Solutions* 17 February 2012. Online at: http://www.cloudsolutions.co.uk/cloud-computing/google-and-data-protection-act-and-fsa-regulations/

"Over a Third of Wall Street and Canary Wharf Workers are Stealing Sensitive Data", Computer Weekly 23 November 2009. Online at: http://www.computerweekly.com/news/1280091445/Over-a-third-of-Wall-Street-and-Canary-Wharf-workers-are-stealing-sensitive-data

"Security Whitepaper: Google Apps Messaging and Collaboration Products", Google 2011. Online at: https://docs.google.com/file/d/0B5Y-fwYJF2hLOTVmMzQ1MjAtMDFmNS00YjFhLWI3MmUtZjI5MDQ5Mzc3NmMz/edit?hl=en&pli=1

"Verio and Citrix to Power New Cloud Service Offering", *DABCC* 11 April 2012. Online at: http://www.dabcc.com/article.aspx?id=19881

Asser, M (2000), "Echelon: Big Brother Without a Cause?", *BBC* 6 July 2000.Online at: http://news.bbc.co.uk/1/hi/world/europe/820758.stm

Barrington, M, "Eversheds Announces Pilot iPad Programme For Its Lawyers", *iPadLawyer* 2010. Online at: http://ipadlawyer.co.uk/eversheds-announces-pilot-ipad-programme-for

Binning, D (2009), "Top Five Cloud Computing Security Issues", *Computer Weekly* 24 April 2009. Online at: http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm

Brodkin, J (2008), "Gartner: Seven Cloud Computing Security Risks", *InfoWorld* 2 July 2008. Online at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1

Byrne, M (2011), "Clifford Chance and Microsoft Plan New Dawn for Legal IT", *The Lawyer* 17 January 2011. Online at: http://www.thelawyer.com/clifford-chance-and-microsoft-plan-new-dawn-for-legal-market-it/1006630.article

Citrix XenApp guidance. Online at: http://www.1st-computer-networks.co.uk/citrix_xen_app.php

Gasior, G (2010), "An Evening with OnLive's Cloud Gaming Service", *The Tech Report* 15 October 2010. Online at: http://techreport.com/discussions.x/19813

Google, "Google Apps for Business: Benefits". Online at: http://www.google.com/enterprise/apps/business/benefits.html

Graham, I (2010), "Personal Information Online Code of Practice", *Information Commissioner's Office* July 2010. Online at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf

Hickey, A (2010), "SMB Cloud Spending to Approach $100bn By 2014", *Channelweb*. 19 August 2010. Online at: http://www.crn.in/Software-019Aug010-SMB-Cloud-Spending-To-Approach-100-Billion-By-2014.aspx

Information Commissioner's Office, "Sending Personal Data Outside The European Economic Area", *Information Commissioner's Office*. Online at: http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_8

ISO (2007), "An Introduction to ISO 27001", *International Standards Organisation* 2007. Online at: http://www.27000.org/iso-27001.htm

Levy, S (2012), “Google Throws Open Doors to its Top Secret Data Centre”. *Wired*, 17 October 2012. Online at: http://www.wired.com/wiredenterprise/2012/10/ff-inside-google-data-center/all/

Linder, B (2008), “Wuala: Peer to Peer Online File Storage and Sharing”, *Download Squad* 14 February 2008. Online at: http://downloadsquad.switched.com/2008/02/14/wuala-peer-to-peer-online-file-storage-and-sharing/

Mitchell, L (2010), “ICO Slaps £100,000 Fine on Herts CC for Data Lapse”, *Public Technology* 24 November 2010. Online at: http://www.publictechnology.net/sector/local-gov/ico-slaps-100000-fine-herts-cc-data-lapse

Moazzezi, O (2012), “How Secure is the Cloud?”, *Computer Technology Review* 5 March 2012. Online at: http://wwpi.com/index.php?option=com_content&view=article&id=14353:how-secure-is-the-cloud&catid=322:ctr-exclusives&Itemid=2701741

Morin, M, “What is Cloud Computing? Interviewing Dave Vandervort of Xerox Innovation Group”, *Ruby About.com*. Online at: http://ruby.about.com/od/cloudcomputing/a/dvandervort.htm.

Parry, S (2010), “Cloudy and Bright—a Case Study from Virtual Practices”, *Legal Futures* 21 December 2010. Online at: http://www.legalfutures.co.uk/practice-points/technology/cloudy-and-bright-%E2%80%93-a-case-study-from-virtual-practices.

Rash, K (2011), “Stuxnet Turns USB Memory Sticks into Weapons of Mass Destruction”, *Eweek* 16 February 2011. Online at: http://www.eweek.com/c/a/Security/Stuxnet-Turns-USB-Memory-Sticks-into-Weapons-of-Mass-Destruction-334848/

Shane, D (2010), “Exposed on the Internet”, *Information Age* 14 October 2010. Online at: http://www.information-age.com/channels/security-and-continuity/perspectives-and-trends/1290833/exposed-on-the-internet.thtml

Shrimanker, H (2009), “Timeline and History of Software as a Service (SAAS)”, *Merinews* 7 May 2009. Online at: http://www.merinews.com/article/timeline-and-history-of-software-as-a-service-saas/15768349.shtml

Tey, L (2011), “Cloud Customers Risk Collateral DDOS”, *SC Secure Business Intelligence* 24 February 2011. Online at: http://www.securecomputing.net.au/News/249231,cloud-customers-risk-collateral-ddos.aspx

Tisnovsky, R (2010), “Risks Versus Value in Outsourced Cloud Computing”, *Financial Executive* 1 November 2010. Online at: http://business.highbeam.com/388/article-1G1-243279222/risks-versus-value-outsourced-cloud-computing

Travis, A (2008), “Consultants Pay Price after Prisoner Data Loss”, *The Guardian*, 11 September 2008. Online at: http://www.guardian.co.uk/politics/2008/sep/11/justice.security

Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (“USA PATRIOT”) Act 2001 (USA). Online at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Van der Zwet, J (2012), “Layers of Latency: Cloud Complexity and Performance”, *Wired*, 18 September 2012. Online at: http://www.wired.com/cloudline/2012/09/layers-of-latency/

Whittaker, Z (2011), “Microsoft Admits US Patriot Act Can Access EU Based Cloud Data”, *ZDNet* 28 June 2011. Online at: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225