Chapter 6: Cloud Computing *

1. Introduction

Cloud computing technology promises to revolutionise business models for data processing, dissemination and storage, through on-demand, low cost, Internet-based computing services. Indeed, analysts estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12 per cent of the worldwide software market will move to the cloud in that period.[1] However, unless companies providing or using cloud computing models can adequately reassure individuals that their data will be accessible and the privacy of their data will be safeguarded, consumers may not permit their data to be processed in this way, and businesses may find themselves constrained in their choices of IT services.[2] This chapter begins by exploring the technological and business capabilities of cloud computing before examining the contractual, privacy and data protection concerns generated by this advance in computing, and assessing the adequacy of current EU laws, in order to determine whether the promised cloud computing economic silver linings are threatened by legal storm clouds.

1.1 What is cloud computing?

> Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased.[3]

There is, as yet, no universally accepted definition of cloud computing; it is in fact an umbrella term which covers a range of computing technologies.[4] Vaquero et al. analysed a variety of definitions proposed in literature in order to provide an integrative definition:

---

1. P. Bruening and B. Treacy, 'Cloud Computing: Privacy, Security Challenges', *Privacy and Security Law Report*, 8(10) (2009), 2.
2. P. Treacy and B. Bruening, 'Cloud Computing: Data Protection Concerns Unwrapped', *Privacy and Data Protection*, 9(3) (2010), 13.
3. M. Armbrust, A. Fox, et al. (2009) 'Above the Clouds: A Berkeley View of Cloud Computing', http://radlabs.cs.berkeley.edu, last accessed 17 June 2009.
4. L. Youseff, M. Butrico, et al., 'Toward a Unified Ontology of Cloud Computing', Grid Computing Environments Workshop, 2008. GCE '08 http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf, last accessed 12 June 2009.

* Karen Mc Cullagh is a lecturer at Salford University. Her research focuses on the privacy and data protection implications of emerging technologies. She may be contacted via: k.mccullagh@salford.ac.uk.

> Clouds are a large pool of easily usable and accessible virtualised resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure provider by means of customized SLAs (Service Level Agreements).[5]

Thus, the cloud is a metaphor for the Internet, as the term cloud computing refers to Internet-based software that allows users to remotely access services without the need to control the infrastructure that provides the services. Although the underlying technology is not new, the use of it in this way is novel, in that

> We're moving into the era of 'cloud' computing, with information and applications hosted in the diffuse atmosphere of cyberspace rather than on specific processors and silicon racks. The network will truly be the computer.[6]

Johnson, et al.[7] observe that cloud-based applications do not, therefore, run on a single computer; instead they are spread over a distributed cluster, utilising computing resources and storage space from as many available machines as are needed,[8] and are not tied to a particular location or owner, though many companies have proprietary clouds. For instance, Amazon's cloud[9] refers to the computers used to power Amazon.com; the capacity of those servers has also been harnessed as the 'elastic compute cloud' (EC2)[10] and can be leased from Amazon for a variety of purposes. Thus, clouds may be described as 'public' or 'private.' Armbrust et al[11] define *Public* clouds as utility computing services which are available on a pay-as-you-go basis to the general public, whereas the term 'private' cloud is used to describe the internal data-centres of a business or organisation, not made available to the general public. This chapter focuses on public cloud services and the issues which different sized enterprises should be cognisant of when contracting for cloud services. It illustrates how small- and medium-size enterprises (SMEs) (unlike large enterprises, whose legal counsel

---

5. L. Vaquero, L. Rodero-Merino, et al., 'A Break in the Clouds: Towards a Cloud Definition', ACM Computer Communication Reviews, 2009.
6. E. Schmidt, 'Don't Bet against the Internet', *Economist*, 16 November 2006, http://www.economist.com/theworldin/business/displayStory.cfm?story_id=8133511&d=2007 (registration required), last accessed 12 June 2009.
7. L. Johnson, et al., 'The 2009 Horizon Report', Austin, Texas: The New Media Consortium, 2009.
8. *The Cloud* is conceptually similar to the term 'Telecom cloud', used to describe a type of networking in telephony. Until the 1990s, data circuits (including those that carried Internet traffic) were hard-wired between destinations. Subsequently, long-haul telephone companies began offering Virtual Private Network (VPN) service for data communications. These offered the same guaranteed bandwidth as fixed circuits, but at a lower cost because they could switch traffic to balance utilization as they saw fit, thus utilizing their overall network bandwidth more effectively. As a result of this arrangement, it was impossible to determine in advance precisely paths traffic would be routed over.
9. Amazon Web Services is an example of a proprietary cloud which is publicly available: http://www.aws.amazon.com, last accessed 2 August 2009.
10. Amazon Elastic Compute Cloud (Amazon EC2): http://aws.amazon.com/ec2/, last accessed 20 June 2009.
11. Armbrust, Fox, et al., 'Above the Clouds: A Berkeley View of Cloud Computing',

specifically draft tailor-made contractual clauses) are typically presented with standard form contracts containing non-negotiable terms and conditions, thereby potentially exposing them to liability for data protection and security risks which must be borne in mind when deciding whether to avail of cloud computing services.[12]

1.2 Cloud components

Cloud computing comprises two elements, namely: 'cloud software services' and 'cloud computing services'. Cloud software services, commonly referred to as 'Software as a Service' (SaaS)[13] comprises a variety of business, consumer and prosumer[14] services. The SaaS vendor provides the software applications as well as the computing power, storage, and networking infrastructure necessary to run the application by deploying a virtual machine.[15] Key features of SaaS are that complete applications are available over the Internet on demand and the end user does not need to pay for software or support the infrastructure that applications run upon.[16] Examples of SaaS offerings include: salesforce.com,[17] a CRM system for use in sales administration; likewise, Google Apps is SaaS which offers word processing, spreadsheet, and presentation applications as well as e-calendars, email and Netsuite (a CRM package that also offers accounting, ERP[18] and electronic commerce functionality).[19]

Cloud Computing Services splits into 'Platform-as-a-Service' (PaaS) and 'Infrastructure-as-a-Service' (IaaS). PaaS is the delivery of a computing platform and solution stack as a service. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers,[20] providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet[21] with no software downloads or installation for developers, IT managers or end-users. An example of a PaaS offering is that of Salesforce in the form of force.com, through which a platform is made available through the web to developers, so that they can customise the application to meet the particular needs of their

12. The contractual terms of private cloud services are individually negotiated and are tailored to meet the needs of the customer, and accordingly are more easily managed by the organisation's IT personnel.
13. Increasingly analysts are separating this out from cloud computing.
14. A portmanteau of producer and consumer.
15. The SaaS vendor may utilise a third party IaaS or PaaS vendor to provide the compute power, storage, and networking infrastructure but this does not always have to be the case. The application may be implemented in such a way that it directly consumes resources without the need for third party infrastructure services or platform services.
16. The pricing structure for *SaaS* is usually a per user per month fee.
17. Salesforce.com: http://www.salesforce.com, last accessed 17 June 2009.
18. Enterprise resource planning (ERP) is a company-wide computer software system used to manage and coordinate all the resources, information, and functions of a business from shared data stores.
19. Examples of usages: If a business's CRM package is not managing the load or they simply don't want to host it in-house, then they could use a SaaS provider such as Salesforce.com. Another example is a business outsourcing their email to the cloud, rather than run it on internal exchange servers.
20. J. Schofield, 'Google angles for business users with 'platform as a service', *Guardian*, 17 April 2008, http://www.guardian.co.uk/technology/2008/apr/17/google.software, last accessed 20 June 2009.
21. D. Hinchcliffe, 'Comparing Amazon's and Google's Platform-as-a-Service (PaaS) Offerings', 11 April 2008, http://blogs.zdnet.com/Hinchcliffe/?p=166&tag=btxcsim, last accessed 20 June 2009.

users, or indeed develop the platform to meet entirely new requirements. This is a particular strength, as traditional platforms are built upon infrastructure, which is expensive, because estimating demand is not an exact science.[22]

'Infrastructure as a Service' (IaaS) is the delivery of computer infrastructure as a service. Rather than purchasing servers, data centre space or network equipment etc., clients instead contract to purchase the required resources as a fully outsourced service. IaaS allows these capabilities to be turned on and off at will, and customers are only charged for what they use when they use it (similar to utility billing structures). The most widely recognised example of IaaS is Amazon Web Services,[23] where the infrastructure and computing skills originally developed to underpin the Amazon Internet bookseller business model are now deployed in a generalised, non-sector specific offering to the world at large.[24]

2. Utopian promise of Cloud computing: the sky's the limit

The economic case for investing in cloud computing as an essential component of the digital economy was outlined by the EU Commissioner for Information Society and Media when she stated:

> Europe's digital economy should be opened up to small businesses. In Europe, we have 23 million small and medium sized enterprises (SMEs) which make up 99% of all firms. Accounting for over 100 million jobs, SMEs can be the mainspring of Europe's economic resurgence. But in the use of productivity-boosting ICT tools, SMEs lag substantially behind big firms: only 9% of SMEs use electronic invoices, and only 11% of them have technology-based human resource management. If SMEs could access computing power over the web, they would no longer need to buy and maintain technologies or IT applications and services. Such web-based services – called "cloud computing" – are the medicine needed for our credit squeezed economy: they can make businesses more productive by shifting from fixed costs (i.e. hiring staff or buying PCs) to variable costs (i.e. you only pay for what you use).[25]

Thus, as a business model, cloud computing offers numerous benefits to SMEs because they do not have to invest in new infrastructure, manage computer systems and servers, provide security measures, updates and back-ups, licence new software, or employ IT support staff.

---

22. Examples of PaaS usage: a University needs to host a large file (10Mb) on their website and make it available for 1000 users during the two-month period of a summer school. It could use Cloud Front from Amazon. Another example is an organisation that wants to start storage services on its network for a large number of files but does not have the storage capacity, e.g. a law firm that wishes to store their client's records. It could use Amazon S3.
23. Amazon Web Services: http://aws.amazon.com/, last accessed 7 July 2009.
24. Examples of *IaaS* usage: A business wants to run a batch job but they don't have the infrastructure necessary to run it in a timely manner. They could use Amazon EC2. Another example is an organisation that wants to host a website, but only for a few days, e.g. for the sale of music festival ticket sales. They could use Flexiscale.
25. V. Reding, 'Digital Media - Europe's Fast Track to Economic Recovery', The Ludwig Erhard Lecture 2009, Lisbon Council, Brussels, 9 July 2009, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/336&format=HTML&aged=0&language=EN&guiLanguage=en, last accessed 24 August 2010.

The economic need for this is supported by research conducted by Gartner[26] which found that approximately two-thirds of the average corporate IT staffing budget is spent on support and maintenance activities. Indeed, Treacy and Bruening posit that cloud computing promises computing system and economic changes for businesses since:

> Freed from the need to buy service and maintain their IT infrastructure, businesses will become more nimble, better able to adapt to changing market demands, and to take advantage of services more effectively and economically provided by others.[27]

This model of computing offers a number of benefits, including:

Little or low initial investment: the norm is for cloud computing customers not to own the physical infrastructure acting as host to the software platform in question. Thus, they avoid capital expenditure on hardware, software, and services by renting provision from a third party provider.

> Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue.[28]

This lowers barriers to entry, and has ongoing benefits in the sense that infrastructure does not need to be purchased for single or infrequent intensive computing tasks.

Reduced running costs: Consumption is billed on a utility (e.g. resources consumed, like electricity) or subscription (e.g. time-based, like a newspaper) basis with little or no upfront cost, saving organisations money. These cost savings are achieved by 'following the moon'[29] a metaphor which describes how the cloud service providers transfer data to different locations according to the cost of electricity, as in general electricity costs are lower at night since there is less demand when people are asleep, and also because the temperature is lower and so cooling costs are cheaper. Thus, companies run applications from wherever in the world and at whatever time of day cheaper resources are available.

Scalability: Macqaurie Telcoms[30] contend that one of the key features of cloud computing

---

26. B. Gomolski, 'U.S. IT Spending and Staff Survey', Gartner Research, Stamford, CT (2005).
27. Treacy and Bruening, 'Cloud Computing: Data Protection Concerns Unwrapped', p, 13.
28. Armbrust, Fox, et al., 'Above the Clouds: A Berkeley View of Cloud Computing'.
29. H. Wagter, 'Follow the Moon', daDa Motive: On the edge of change, 21 July 2009, http://www.dadamotive.com/2009/07/follow-the-moon.html, last accessed 4 August 2009.
30. Macquarie Telecom, 'The Business perspective on Cloud Computing', 25 May 2009, http://www.macquarietelecom.com/hosting/blog/Cloud_Computing_Position_Paper.pdf, last accessed 24 August 2010.

services is the ability to flex by increasing or decreasing provision on-demand. This capability allows a business to manage fluctuations in demand in real time, without needing to invest in capacity to meet peak demand. As a result, meeting demand spikes and batch processing jobs is no more expensive than meeting normal demand

> Companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT.[31]

Cloud computing therefore offers much more flexibility and efficiency than past computing methods.

Data Portability and security: Since infrastructure is located off-site and accessed via the Internet the users can connect from anywhere, regardless of the connection device used e.g. mobile, PC

> The desktop is dead. Welcome to the Internet cloud, where massive facilities across the globe will store all the data you'll ever use.[32]

Thus, employees can access information wherever they are, rather than having to remain at their desks. Also, the user does not have to carry, or be responsible for, storage devices (e.g. USB drives, CDs etc.) thereby potentially increasing data security.

In summary, access to data anywhere anytime, cost savings[33] and a reduced burden of running and maintaining IT infrastructure are key features that make cloud sourcing attractive, as organisations are freed to concentrate on innovation and profit-making opportunities.

Storm clouds: Data (in)accessibility and opaque Service Level Agreements

However, in the short history of cloud computing there have been a number of server outages. For instance, in October 2009, Sidekick temporarily lost the data of T-mobile customers due to server crash.[34] Each outage has resulted in cloud users being unable to access their data for varying lengths of time. Such outages can have severe repercussions for service users, both in terms of lost revenue and disappointed customers. Thus, organisations who are contemplating contracting for cloud service provision should be advised to review the terms of the Service Level Agreements available, as they typically state the law which governs the contract and the competent in case of disputes arising from the interpretation and/or the

31. Armbrust, Fox, et al., 'Above the Clouds: A Berkeley View of Cloud Computing'.
32. G. Gilder, 'The Information Factories', *Wired*, 14(10) October 2006, http://www.wired.com/wired/archive/14.10/cloudware_pr.html, last accessed 12 June 2009.
33. There are also arguments that this can reduce a business's carbon footprint.
34. Network World Staff, 'From Sidekick to Gmail: A Short History of Cloud Computing Outages', *Network World*, 12 October 2009, http://www.networkworld.com/news/2009/101209-sidekick-cloud-computing-outages-short-history.html?fsrc=netflash-rss. This article details other cloud computing outages.

execution of the contract, e.g. compensation for server outages, data losses, etc. Although the parties entering into a contract for cloud service provision are free to negotiate the terms of their own service level agreement, this option will typically only be used by large organisations that have equality of bargaining power. In contrast, many SMEs will simply not be able to negotiate on equal terms with the cloud service providers, and as a result, they may accept the SLA terms unilaterally drafted by the supplier. Such terms are likely to be drafted in the provider's favour. For example, the Customer Agreement for Amazon Web Services states:

> We and our licensors do not warrant that the service offerings will function as described, will be interrupted or error free, or free of harmful components, or that the data you store within the service offerings will be secure or not otherwise lost or damaged. We and our licensors shall not be responsible for any service interruptions, including, without limitation, power outages, system failures or other interruptions ... [35]

A content analysis was conducted of the SLAs of five of the market leaders in cloud computing. Google Apps SLA states that the parties will be bound by the laws of the State of California[36] whilst the terms of service of Amazon's SLA states:

> By using the Services, you agree that the laws of the State of Washington, without regard to principles of conflicts of laws, will govern this Agreement and any dispute of any sort that might arise between you and us. The parties expressly exclude application of the United Nations Convention for the International Sale of Goods to this Agreement.[37]

Where the SLA contains a choice of law clause the law governing the contract will be that chosen by the parties.[38] In contrast, the SLAs of GoGrid and Microsoft Azure are silent regarding applicable laws. Where the SLA is silent as to choice of law, Rome I Regulation[39] stipulates that the law of the country with which the contract is most closely connected is applicable. Accordingly, the place of performance of the obligation (and therefore the competent court) will generally be determined under the law of the country where the cloud service supplier has its central administration; yet this is difficult to determine when cloud computing involves transnational data transfers.

The choice of laws may have serious repercussions for SMEs. For instance, a French gift shop that contracts for the provision of cloud services by Amazon to manage high volume,

---

35. Amazon Web Service Customer Agreement, 7 July 2010, Section 11.5, http://aws.amazon.com/agreement/.
36. Google Terms of Service, http://www.google.com/apps/intl/en/terms/premier_terms.html, 15.10 'Governing Law'. 'This Agreement is governed by California law, excluding that state's choice of law rules. For any dispute relating to this agreement, the parties consent to personal jurisdiction in, and the exclusive venue of, the courts in Santa Clara County, California.'
37. Amazon SLA, http://aws.amazon.com/agreement/#14, 14.2, 'Governing Law'.
38. Art. 3 of the Rome Convention.
39. Rome I Regulation, regulates choice of laws for contracts entered into after 17 December 2009. Regulation (EC) No 593/2008 of the European Parliament and the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (OJ L177, 4 July 2008, pp. 6–16).

but intermittent order demands (e.g. to manage Christmas gift supply and distribution) would be deemed to be a business, and the contract with the cloud service provider would be a Business to Business (B2B) SLA.[40] However, if problems arise, e.g. if the cloud service provider's servers suffers an outage during peak demand times affecting the Gift Shop's ability to process orders in the period before Christmas, it could suffer huge financial losses, but not be able to afford the inconvenience and expense of enforcing their rights in another country or continent, namely the USA.[41]

As a result, Parrilli[42] advocates amending legislation to classify SMEs as consumers when they enter into SLAs with cloud service providers. If so, the SLA would be regulated by the law of the country where the SME consumer has their habitual residence if the cloud provider addresses this country through a website/portal. This would reduce costs for a SME if they needed to litigate. Furthermore, the parties would still be free to agree that another law (e.g. of a USA state) will govern the contract, but consumer protection rules of the country of residence of the consumer would still apply.[43] Thus, classifying a SME as a consumer would be advantageous as it would reduce the cost and complexity of bringing legal proceedings against a cloud provider which breaches a service level agreement.

3.2 Privacy and data protection storm clouds

In addition to data inaccessibility problems, many potential cloud users are concerned about the security and privacy of their data:

> ...the cloud demands a high degree of trust. Significant amounts of data which were previously stored only in individual offices and homes would now reside in data centres controlled by third parties.[44]

If companies providing or using cloud computing models cannot adequately reassure individuals that their data will be safeguarded, consumers may not permit their data to be processed in this way, and businesses may find themselves constrained in their choices of IT services.[45] In 2008, a Pew Internet & American Life Project study conducted survey research on the attitudes of the American Public to potential cloud services: see Table 6.1.

---

40. In contrast, a gift shop owner who bought cloud storage capacity for their personal files, e.g. photo albums, music collection, etc, would be deemed to be a consumer.
41. C. Wild, et al., 'Council Regulation (EC) 44/2001 and Internet Consumer Contracts: Some Thoughts on Article 15 and the Futility of Applying "In the Box" Conflict of Law Rules to the "Out of Box" Borderless World', *International Review of Law, Computers & Technology*, 19(1) (2005).
42. D. Parrilli, 'The Determination of Jurisdiction in Grid and Cloud Service Level Agreements', GECON, vol. 5745 (2009) of Lecture Notes in Computer Science, pp. 128–39.
43. e.g. Directive 93/13/EC of 5 April 1993 on unfair terms in consumer contracts [OJ L95, 21.4.1993, pp. 29–34].
44. A. Weiss, 'Computing in the Clouds', *netWorker*, 11(4) (2007), p. 25.
45. Treacy and Bruening, 'Cloud Computing: Data Protection Concerns Unwrapped', p. 13.

(See original table for display/formatting guidance)

Table 6.1 **Attitudes about possible data policies of 'cloud' services**

Thinking about your data, such as email, photos, and other files that you put on these online services, how concerned, if at all, would you be if companies that provide these services...

	Level of concern			
Action	Very	Somewhat	Not too	Not at all
	(% using online applications and services to store data)			
Sold your files to others	90	5	2	3
Used your photos and other information in marketing campaigns	80	10	3	6
Analysed your information and then displayed ads to you that are based on what you have in those files	68	19	6	7
Kept a copy of your files even if you delete them	63	20	8	8
Gave law enforcement agencies your files when asked to do so	49	15	11	22

Source: J. B. Horrigan, 'Use of Cloud Computing Applications and Services', Data Memo, Pew Internet and American Life Project (2008), http://pewinternet.org/pdfs/PIP_Cloud.Memo.pdf, p. 2. Pew Internet & American Life Project April-May 2008 Survey N=999 for those who have used online services to store personal information. Margin of error is ± 3.5%.

Table 6.1 reports high levels of concern among American public cloud users when presented with scenarios in which companies may put their data to uses of which they may not be aware. For instance, 90 per cent of cloud application users indicated that they would be very concerned if the company at which their data were stored sold it to another party. Also, 80 per cent would be very concerned if companies used their photos or other data in marketing campaigns, and 68 per cent of users stated that they would be very concerned if companies who provided cloud computing services analyzed their information and then displayed advertisements to them based on their actions.

Moreover, these concerns appear to be justified: in 2007 the cloud service provider Salesforce.com sent a letter to a million subscribers advising that customer emails and addresses had been stolen by cybercriminals.[46] Also, in 2009 the security of Google Apps was breached by a cracker who hacked into the Gmail account of a Twitter employee and threatened to publicly expose commercially sensitive information.[47] Unless such concerns are managed, individuals may not permit organisations to use cloud services when processing their data.

46. A. Greenberg, 'Cloud Computing's Stormy Side', *Forbes Magazine*, 19 February 2008, http://www.forbes.com/2008/02/17/web-application-cloud-tech-intel-cx_ag_0219cloud.html, last accessed 8 July 2009.
47. C. Marwitz, 'Twitter Hack A Google Problem? Or Blame Cloud Computing?', 16 July 2009, http://windowsitpro.com/Articles/Index.cfm?ArticleID=102490&feed=rss&subj=0, last accessed 2 August 2009.

Table 6.2:

Key elements of privacy policies

Cloud Service Provider	Visitor/ User Tracking	Retention of Visitor/ User data	Usage of cookies/ web beacons[a]	User notified of changes to privacy policy
Amazon S3 & Simple DB[b]	Yes	No Information	Yes	Only if materially different
GoGrid[c]	Yes	Yes	No Information	Yes
Google apps[d]	No Information	No Information	Yes	Only if materially different
Microsoft Azure[e]	Yes	No Information	Yes	Only if materially different
Salesforce[f]	Yes	Account closing information provided	Yes	No

Notes:
a. 'What are web beacons (also known as 'web bugs') and clear GIFs?' www.allaboutcookies.org/web-beacons/index.html (accessed 7 July 2009).
b. Amazon.com Privacy Policy www.amazon.com/gp/help/customer/display.html/190-9616536-9048729?ie=UTF8&nodeId=468496 (accessed 7 July 2009).
c. GoGrid Privacy Policy www.gogrid.com/legal/privacy-policy.php (accessed 21 October 2009)
d. Google apps index page www.google.com/apps/; Privacy policy www.google.com/privacypolicy.html (accessed 7 July 2009).
e. Microsoft Privacy Policy http://privacy.microsoft.com/en-us/fullnotice.mspx (accessed 7 July 2009).
f. Salesforce Privacy Policy www.salesforce.com/company/updated_privacy.jsp (accessed 7 July 2009).

Note Table 6.2 is in wrong position

3.2.1 **Compliance with EU Directive 95/46/EC**

One way in which cloud computing providers can seek to promote and maintain confidence of EU citizens in their services is through compliance with Directive 95/46/EC when processing individuals' data. Three of the eight data protection principles in the Directive are pertinent in relation to cloud computing, namely, the First, Seventh and Eighth principles.

3.2.2. *First principle: lawful processing of personal data*

Cloud computing providers can comply with the first principle through the adoption of appropriate terms of service and robust privacy policies. To date, cloud providers have typically utilised standard terms rather than individually negotiated contracts.[48] Thus, there is an obvious need to examine their standard form contract terms, service level agreements and privacy policies in detail, to ascertain whether they comply with EU data protection laws. A content analysis was conducted of the policies of a sample of five of the market leaders[49] in cloud computing (see Table 6.2).

Insert Table 6.2 here.

48. This paper is concerned only with issues pertaining to public clouds since contracts for such services will typically contain standardised terms of use and service level agreements which may not provide adequate data protection assurances to cloud service users (in contrast with a private cloud, where the parties can negotiate contract terms).
49. J. Brodkin, '10 cloud computing companies to watch', *Industry Standard*, 17 May 2009, http://www.thestandard.com/news/2009/05/17/10-cloud-computing-companies-watch?page=0%2C0, last accessed 7 July 2009.

Of the five policies analysed, Table 6.2 indicates that the majority indicated that users/visitors would be tracked so that non-personal, transactional information could be collected. Similarly, four of the five providers use cookies or web beacons; a few stated that cookies may be disabled, but warned that doing so would reduce the site's functionality or accessibility, as the site could not be modified or targeted towards a particular visitor or user's preferences. All privacy policies analysed indicated that they reserved the right to change the terms and conditions at will, and that any changes to the policy would be notified on the cloud service provider's website, thereby placing the onus on the user to periodically review the website and check for updates. Only three of the five companies promised to notify users in advance if material changes were to be made to the policy, by emailing them. Significantly, all cloud service providers expected users to check the privacy policies of third parties e.g. advertisement suppliers, with whom there may be an interaction as a result of accessing the cloud service provider's website. Whilst this approach may be cost-effective for cloud service providers, it is not likely to reassure users who would prefer to be informed directly, by email of changes to the privacy policy.

3.2.3 *Seventh principle: Data must be kept secure*

As alluded to earlier, the term cloud computing is, in one respect, a misnomer because

> Behind all the rhetoric and promotional guff the 'cloud' is no such thing: every piece of data is stored on a physical hard drive or in solid state memory, every instruction is processed by a physical computer and every network interaction connects two locations in the real world.[50]

Cloud computing data is not therefore stored in the empyrean sphere; rather it is stored on computer servers. This raises the issue of data security as the *seventh* data protection principle states:

> appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing or accidental loss or destruction of personal data.

Abadi[51] asserts that moving data off premises increases potential security risks, as a cloud computing provider could violate the privacy of its customers and access data without permission. Also, there is a possibility that system errors may produce unintentional leaks of information from one customer to another. For instance, as a result of a flaw in the Google Docs application, some users inadvertently shared some of their documents.[52] Under Directive 95/46/EC the data controller remains responsible for personal data, even where the data are

---

50. B. Thompson, 'Storm warning for cloud computing', *BBC News*, 27 May 2008, http://news.bbc.co.uk/1/hi/technology/7421099.stm, last accessed 2 August 2009.
51. D. Abadi, 'Data Management in the Cloud: Limitations and Opportunities', Bulletin of the IEEE Computer Society Technical Committee on Data Engineering (2009).
52. D. Raywood, 'Google admits that some of its Docs have been accidentally shared', *S C Magazine*, 10 March 2009, http://www.scmagazineuk.com/Google-admits-that-some-of-its-Docs-have-been-accidentally-shared/article/128491, last accessed 20 October 2009.

processed by a third party, and so it requires the controller to ensure that any third party processing personal data on its behalf takes adequate technical and organisational security measures to safeguard the data. European data protection law requires a contractual provision between the controller and processor to this effect, and controllers typically seek to monitor whether this obligation is fulfilled by undertaking an audit or conducting due diligence inquiries.[53] Tracey & Bruening[54] opine that obtaining data security assurances presents significant challenges, especially where the cloud vendor is small or unproven, since smaller vendors based outside Europe may not even be aware of the requirements of the Directive. Moreover, cloud computing inherently poses greater risks than traditional desktop-based or enterprise computing because the data is beyond the physical control of the data controller. This has led to calls for cloud computing services to be forced to adopt increased security features such as mandatory encryption of all stored consumer data. However, there is an ongoing debate about whether this is feasible. Reingold & Mrazik[55] argue that encryption is not a panacea to all cloud computing security issues as although cloud computing service providers offer encryption services during data transmission, a request for encryption of stored data would go beyond the industry standard and might, because of technological constraints, degrade the services.[56] Also, Mowbray[57] suggests that since data generally has to be unencrypted at the point of processing (i.e. if it is processed using cloud computing) it will generally be present in unencrypted form on a machine in the service provider or subcontractor's network. There is, therefore, a risk of theft or sabotage by a rogue employee of the service provider or subcontractor, and a need for technological protections to prevent customers (who may be commercial rivals) from spying on each others' data or interfering with each others' computations.

Eighth principle: Transfers to countries with 'adequate' data protection

Transnational data transfers are the norm in cloud computing environments. For instance, an individual living in France could purchase a book via the Amazon.fr website. However, the book order could be processed from any of its numerous data centres e.g. Ireland, whilst the book could be dispatched from a warehouse in the USA. Customer data could be sent at the end of the trading day to Singapore, and archive data could be sent to a separate, undisclosed

53. Similarly, in the USA, the Federal Trade Commission has used its authority under the unfairness prong of the FTC Act's Section 5 in enforcing the Safeguard Rule of the Gramm-Leach-Bliley Act to determine whether a company's information security measures were reasonable and appropriate under the circumstances. The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information.
54. Treacy and Bruening, 'Cloud Computing: Data Protection Concerns Unwrapped', p.13.
55. B. Reingold and R. Mrazik, 'Cloud Computing: The Intersection of Massive Scalability, Data Security and Privacy (Part I)', *Cyberspace Lawyer*, 14(5) (2009), 2.
56. N. Roiter, 'How to Secure Cloud Computing', *Information Security Magazine*, March 2009, http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349670,00.html, last accessed 21 June 2009, indicates that all service providers offer strong encryption during transmission, but that encrypting data at rest is more complex); see e.g. Zoho.com, 'Zoho Security Practices, Policies and Infrastructure', http://www.zoho.com/security.html (discussing encryption during transmission, but not while data is at rest), last accessed 21 June 2009.
57. M. Mowbray, 'The Fog over the Grimpen Mire: Cloud Computing and the Law', *Script-Ed*, 6(1) (2009) p136.

(for security purposes) location. A single customer transaction could, therefore, result in the transfer of data across several different countries, and legal jurisdictions. Hence, cloud data centre location is important when assessing the suitability of a cloud service provider, since any information stored in the cloud eventually ends up on a physical machine in a specific country and is subject to the laws of the country where the machine is located. This raises the key issues of which country or countries, the data is processed in, and are their data protection laws 'adequate' if they are beyond the EEA, as the Eighth principle states that:

> personal data must not be transferred to a country outside of the European Economic Area (EEA) unless that country ensures an adequate level of data protection.

As a precaution, some countries are restricting or limiting the use of cloud clients, e.g. France has banned government officials from using Blackberry devices[58]because Blackberries send and receive email using a small number of servers in the USA and UK, and the French security service fears that the risk of data interception poses a threat to national security.[59] Also, the Canadian provincial governments of British Columbia and Nova Scotia require public bodies and their cloud service providers to ensure that personal information under their control is stored and accessed only in Canada, unless specified exceptions apply.[60] Whilst this is the easiest measure from a legislative perspective, it is not a practicable measure for those organisations who engage in transnational business operations.

An analysis of the SLA's, Terms of Service and Privacy Policies revealed that at present, the market leaders in cloud computing are American owned companies, however, some operate data centres in other jurisdictions. Google does not disclose where its data centres are located. It is believed that they do not disclose this information for commercially sensitive reasons, i.e. competitive advantage.[61] This failure to specify data centre locations has implications for users, as a lack of certainty regarding applicable laws has the potential to reduce trust in the Cloud Service provider. Unlike Google, Amazon specifically advertises its decision to locate data centres to respond to different privacy laws; in particular it has 'availability zones' e.g. a data centre in Dublin to meet the needs of EU cloud service providers.[62] Recently, Microsoft announced a decision to also locate a data centre in Dublin, Ireland, though the decision appears to be based on factors such as the cool Irish climate (which reduces operating costs), geographical stability and talent pool, robust Internet connectivity,[63] geological stability,

58. 'Blackberry ban for French elite', *BBC* News, 20 June 2007, http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6221146.stm, last accessed 20 October 2009.
59. Research in Motion, the maker of Blackberries, has denied that there is any risk, 'Blackberry ban for French elite', *BBC* News. Ibid .
60. D. Fraser, 'The Canadian Response to the USA Patriot Act', *IEEE Security and Privacy*, 5(5) (2007), 66–8, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04336282, last accessed 23 March 2009.
61. It is believed that Google has 36 data centres – 19 in the USA, 12 in Europe, three in Asia, one in Russia and one in South America. Google has not substantiated these claims. E. Schonfield, 'Where are all the Google data centres?', TechCrunch, 11 April 2008, http://techcrunch.com/2008/04/11/where-are-all-the-google-data-centers/, last accessed 7 July 2009.
62. R. Wauters, 'Amazon EC2 now available in Europe', TechCrunch, 10 December 2008, http://techcrunch.com/2008/12/10/amazon-ec2-now-available-in-europe/, last accessed 3 August 2009.

proximity to high-speed fibre optic communications networks and affordable energy rates.[64] Whereas, GoGrid's data centre is located in San Francisco, North America, and Salesforce's data centres are located in North America and Singapore. The USA and Singapore are not considered to have 'adequate' data protection measures,[65] thus, *prima facie*, transfers of data to cloud servers in these countries are unlawful. However, on a positive note, Amazon, Google, GoGrid, Microsoft and Salesforce have self-certified compliance with EU Safe Harbour requirements, which *prima facie* permits the transfer of personal data from EU companies to Safe harbour compliant US clouds.[66] Nevertheless, in April 2010, German data protection authorities announced stricter due diligence requirements for the transfer of personal data from the European Union to the United States under the Safe Harbour principles.[67] The requirements are: (i) Safe Harbour certifications which are more than seven years old will generally no longer be considered valid; (ii) the company exporting data to the USA must receive proof from the data recipient how the importing US company is fulfilling its information obligation vis-à-vis the persons affected by the data processing;[68] (iii) companies exporting data must document an examination of compliance provisions and provide this to the supervisory authority upon request. As a result, German companies transferring personal data based upon the Safe Harbour Agreement to the USA are obligated to verify the adherence to the Safe Harbour principles by their contractual partners. If such verification is not possible then the supervisory authorities recommend ensuring the appropriate data protection level by other means, for example, by using model contracts.

Subsequently, the Data Protection Authority of the German Federal State of Schleswig-Holstein published a white paper[69] on cloud computing. The opinions expressed in the paper are not legally binding, but they may influence data protection authorities in other German states.[70] The white paper recommends that companies include contractual provisions governing data controller/data processor relationships regardless of the location of the cloud

63. J. Kirk, 'Microsoft set to fire up Dublin data Center', CIO, 24 September 2009, http://www.cio.com.au/article/319801/microsoft_set_fire_up_dublin_data_center, last accessed 24 September 2009.
64. J. Collins, 'Microsoft opens ?341m data centre in Dublin', *Irish Times*, 25 September 2009, http://www.irishtimes.com/newspaper/finance/2009/0925/1224255210787.html, last accessed 24 September 2009.
65. EU Commission, 'Commission decisions on the adequacy of the protection of personal data in third countries', http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm, last accessed 4 August 2009.
66. Safe Harbour List, http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list?OpenDocument&Start=88, last accessed 4 August 2009.
67. The resolution is available at: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10.pdf.
68. This is important so that the data importer in the USA can pass on the information to the person affected by the transfer.
69. The *Unabhaengiges Zentrum fuer Datenschutz Schleswig-Holstein* – 'ULD' White paper. [Incomplete reference — See email for full reference]
70. Failure to follow the practices in the resolution could potentially lead to an enforcement action by German data protection authorities, as well as reputation damage from negative media attention, which German and US organisations would want to avoid.

computing provider or the services. In addition, companies or qualified external third parties must exert 'regular control' over whether cloud computing providers are complying with data protection requirements. The paper suggests that companies can do this by: obtaining expert advice, in the form of audits or certificates provided by external experts, that the service provider observes the legal restrictions; or they can obtain a binding guarantee declaration by the service provider in which the service provider provides a comprehensive commitment to obeying the obligations imposed by the law.

The approach of some large organisations has been to use model clauses and binding corporate rules to contractually manage the risk associated with international data transfers. However, this approach has been criticised by Tracey as:

> Depending on the location of the vendor's servers, model contracts or safe harbour may not provide a workable solution and, at best, will be cumbersome to implement and maintain. Binding Corporate Rules, on the other hand, remain, at best, a long-term solution for all but the most determined companies.[71]

Accordingly, some organisations are calling for a new data governance model based on 'accountability'. Indeed, Pearson & Charlesworth suggest that cloud computing providers should move away from terms and conditions of service towards accountability contracts between the client and the initial service provider (SP), and between that SP and other cloud providers

> By 'accountability' we mean institutional (inter/intra company) mechanisms that reinforce the (relatively weak) protection that contract law gives to the data subject, thus enhancing trust relationships between corporate processors of PII using cloud computing, and those whose data will be processed.[72]

In effect this approach advocates that businesses actively take ownership of information management by requiring strong contractual assurances from companies providing cloud computing services that they are capable of meeting those obligations and of safeguarding personal data no matter where it is transferred or processed. The advantage of this contractual approach is that it allows an initial service provider to enforce its policies along the chain. As well as having organisational policies, accountability could be supported through 'sticky' electronic data policies.[73]

---

71. Treacy and Bruening, 'Cloud Computing: Data Protection Concerns Unwrapped', p. 14.
72. S. Pearson and A. Charlesworth, 'Accountability as a Way Forward for Privacy Protection in the Cloud', Proceedings, CloudCom 2009, Beijing, Springer LNCS, December 2009, http://www.hpl.hp.com/techreports/2009/HPL-2009-178.pdf.
73. S. Creese, P. Hopkins, et al. 'Data Protection-Aware Design for Cloud Computing', Proceedings, CloudCom 2009, Beijing, Springer LNCS, December 2009, http://www.hpl.hp.com/techreports/2009/HPL-2009-192.pdf. 'Sticky' electronic privacy policies: personal information is associated with machine-readable policies, which are preferences or conditions about how that information should be treated (e.g., that it is only to be used for particular purposes, by certain people or that the user must be contacted before it is used) in such a way that this cannot be compromised. When information is processed, this is done in such a way as to adhere to these constraints. These policies are associated with data using cryptographic mechanisms. The user can be assured that the data processor has correct instructions for each individual data item as to where it may be transferred and processed (e.g. outside of the EEA/Safe Harbour etc).

However, whilst the accountability approach is a useful supplement to Directive 95/46/EC it cannot supplant it, as risks that cannot be addressed contractually will remain. For example, data generally has to be unencrypted at the point of processing, creating a security risk and vulnerability exploitable by cybercriminals. Additionally, only large corporate users are likely to have the legal resources to replace generic SLAs with customised contracts, since adding requirements to the vendor chain will increase the cost of the service.

Conclusion: dispersal of storm clouds

Cloud computing offers revolutionary possibilities by giving individuals and SMEs equality of access to Internet based computing applications and services; thereby allowing them to reduce the operational costs and increase efficiency. However, widespread adoption of cloud computing will not occur until there is a broad-based consensus on standards and protocols regarding data accessibility, and privacy.

Currently, cloud service users experiencing problems regarding level or quality of service provided are expected to rely on SLAs to enforce their contractual rights. However, Parrilli[74] contends that SLAs do not provide adequate reassurances for cloud users as SMEs often have to accept terms and conditions which are unfavourable due to a lack of contractual bargaining power. He advocates that SMEs should be classified as consumers for the purpose of SLAs. However, this approach would be problematic as it would be difficult to draft a definition of when a SME is a consumer as opposed to a business. Another problem with SLAs is that obtaining a decision by a judge does not mean that it will be enforced in non-EU jurisdictions. In concurrence with Parrilli[75] it is suggested that the competent national and international authorities should be encouraged to enter into agreements aimed at facilitating the mutual recognition and enforceability of judgments.

Furthermore, cloud computing raises data protection issues, particularly regarding data storage and trans-national transfers. At present data controllers and data processers seek to discharge their obligations under Directive 95/46/EC through a mixture of model contracts and binding corporate rules. Tracey & Bruening[76] assert that this approach is cumbersome and expensive to administer. Accordingly, there have been calls for existing laws to be supplemented by the adopting an 'accountability'-based data governance model. Pearson[77] opines that this would require data processors to take measures to ensure that the obligations that attach to data – whether through law, company policies or electronic sticky data policies – are met regardless of the jurisdiction in which the information is processed. Until these issues are resolved SMEs should adopt a cautious approach to cloud computing. They should carefully consider whether it is advantageous for them to move their data or functions into the cloud, either in whole or in part. It

74. Parrilli, 'The Determination of Jurisdiction in Grid and Cloud Service Level Agreements'.
75. Ibid.
76. Treacy and Bruening, 'Cloud Computing: Data Protection Concerns Unwrapped', p. 3.
77. S. Pearson, (2009) 'Taking Account of Privacy when Designing Cloud Computing Services', ICSE-Cloud '09, Vancouver. IEEE; Also available as HP Labs Technical Report, HPL-2009-54, http://www.hpl.hp.com/techreports/2009/HPL-2009-54.html, last accessed 24 August 2010.

may be prudent to first test the system with less critical data before using it to process sensitive data. In essence, they must weigh up the financial advantages offered by low cost processing and storage against the potential risk of damage to their reputation if they are associated with data losses or breaches of privacy.