



Queen Mary University of London, School of Law  
Legal Studies Research Paper No. 63/2010

# **Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services**

CN

Simon Bradshaw  
Christopher Millard  
Ian Walden

# Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services<sup>1</sup>

Simon Bradshaw,<sup>2</sup> Christopher Millard<sup>3</sup> and Ian Walden<sup>4</sup>

1 September 2010

## **Abstract**

Cloud computing offers an attractive solution to customers keen to acquire computing infrastructure without large up-front investment, particularly in cases where their demand may be variable and unpredictable. But the greater flexibility of a Cloud computing service as compared with a traditional outsourcing contract is balanced by less certainty for the customer in terms of the location of data placed into the Cloud and the legal foundations of any contract with the provider. This paper reports on a detailed survey and analysis of the Terms and Conditions offered by Cloud computing providers.

## **Keywords**

Cloud Computing, Outsourcing, Data Protection, Information Technology, Contracts, Service Level Agreements, Terms of Service, Terms and Conditions

## **Table of Contents**

1. Introduction
2. Cloud Computing
3. Classifying Cloud Services and Cloud Provider T&C Documents
4. Categorising and Analysing Terms
5. Analysis
6. Conclusions

## **1. Introduction**

The QMUL Cloud Legal Project was set up in late 2009 to identify and evaluate the legal issues arising from the use of Cloud computing.<sup>5</sup> The Project comprises a number of

---

<sup>1</sup> This paper forms part of the Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary, University of London. The authors are grateful to Microsoft for providing generous financial support to make this project possible. The views expressed within this paper, however, are solely those of the authors.

<sup>2</sup> Research Assistant, Cloud Legal Project, Centre for Commercial Law Studies, Queen Mary, University of London.

<sup>3</sup> Professor of Privacy and Information Law and Project Leader, Cloud Legal Project, Centre for Commercial Law Studies, Queen Mary, University of London, and Senior Research Fellow, Oxford Internet Institute, University of Oxford.

<sup>4</sup> Professor of Information and Communications Law, Centre for Commercial Law Studies, Queen Mary, University of London.

distinct workstreams focussing on a range of specific issues; it will produce a series of papers intended to illuminate the legal concerns that providers and users of Cloud services may encounter or wish to be prepared for.

This paper originated in work to gather data regarding the Terms and Conditions (T&C) under which Cloud computing services were offered to customers. This work was initially undertaken to provide background reference material for analysis of specific legal issues associated with Cloud computing, such as privacy, data transfer, third-party access and consumer rights. However, it quickly became apparent that an analysis of Cloud service T&C would not only provide valuable data on which to base such a wider analysis but would also be a substantial and informative research topic in its own right.

The T&C surveyed are those made available or supplied by a range of Cloud service providers. It should be noted that these are standard T&C as offered to customers. In the case of large commercial or Government Cloud contracts, such T&C are likely to be negotiated and tailored to fit the specific requirements of the customer.<sup>6</sup> While certain elements of such bespoke cloud deals may enter the public domain, especially when the customer is a public authority,<sup>7</sup> in general they are unlikely to be made available for analysis. To date, the terms of specific transactions have only been made public in a very few cases. This paper is focussed on, and restricted to, a review of standard T&C.

On initial examination of the various T&C documents obtained from Cloud providers it became clear that many of them follow a pattern in terms of the nature and often the details of the contractual terms offered. An initial overview survey was carried out which highlighted 20 main categories into which T&C elements fell. Each set of T&C was then analysed against these categories. During this process, further patterns emerged. In some categories there was little variation between providers; all or most of them set out very similar terms. In others, a much wider range of approaches was seen. Furthermore, it became apparent that where there was significant variation from provider to provider, the nature of the terms offered were clearly related to the type of service in question, the target market it was aimed at and the commercial legacy of the provider.<sup>8</sup>

It became apparent from the initial survey of T&C that the general form of T&C of a Cloud service could to an extent be predicted in advance from the nature of the service

---

<sup>5</sup> The QMUL Cloud Legal Project is being undertaken by members of the Centre for Commercial Law Studies at Queen Mary, University of London.

<sup>6</sup> At the 2009 Cloud Computing World Europe conference Keryn Ustrup of Moller-Maersk noted that Microsoft had agreed to tailored T&C for a contract to supply Cloud-based email services.

<sup>7</sup> For example, under a public procurement procedure or obtained through a freedom of information request. E.g. the contract between the City of Los Angeles and Google/CSC for the provision of Cloud-based online services may be viewed at <http://www.scribd.com/doc/32676277/City-of-Los-Angeles-and-CSC-Google-Contract>

<sup>8</sup> As will be seen, particularly in areas such as the extent to which a provider disclaims responsibility for failure of a Cloud service, the approach of a provider may reflect the extent to which it has a corporate culture of building long-term trust relationships with its customers.

offered and its target market. This was subsequently borne out in the detailed and comparative analysis of T&C that was undertaken. This paper reports on the results of that work. Given, however, the relative novelty of cloud computing, and the divergence of views as to what it entails, we will first endeavour to clarify what cloud computing is (and, to some extent, is not).

## 2. Cloud Computing

Cloud computing is an increasingly popular approach to providing computing services in a flexible, efficient and readily-accessible manner. Although IT outsourcing has become very common, Cloud computing represents a substantial change in the manner in which organisations and individuals hand over responsibility for the provision of IT infrastructure and services. Traditional IT outsourcing arrangements typically involve negotiated contracts for narrowly specified data storage and processing facilities and services for set periods of time. A customer is likely to deal with a provider directly, and even if the service infrastructure is remote from the customer there will usually be an understanding between provider and customer that a specific set of infrastructure (e.g. servers) has been set aside for the customer's use.<sup>9</sup>

Cloud computing tends to be rather different. The quantity of IT resources procured by the customer may fluctuate over time, often rapidly and dynamically in response to demand. The customer will not normally, other than perhaps in broad geographical terms, be aware of where the service infrastructure is. For all but the largest government and enterprise agreements, the contract will probably be to a standard form and entered into via a routine online process. For these and other reasons Cloud computing raises legal issues beyond those encountered in more traditional IT outsourcing.<sup>10</sup>

A recent report on the future of Cloud computing published by the European Commission<sup>11</sup> identified a number of economic factors that are driving the adoption of a Cloud-based business model; including the following:

- **Cost Reduction:** by sharing resources between a pool of customers and buying infrastructure in bulk, Cloud computing providers can achieve economies of scale that can be passed on to their customers.
- **Transforming CAPEX to OPEX:** moving business operations to the Cloud allows a reduction on capital expenditure on in-house IT infrastructure, which is typically front-loaded and subject to depreciation, in favour of more even ongoing operating expenditure.

---

<sup>9</sup> E.g., M Lewis, 'Information Technology Outsourcing and Services Arrangements', in Reed and Angel (eds.) *Computer Law*, OUP, 2007. Also J Angel (ed), *Technology Outsourcing*, Law Society, 2003.

<sup>10</sup> B Treacy, "Learning to Trust Cloud Computing" (2009) 20(2) *Computers and Law*.

<sup>11</sup> 'The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010', <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>.

- Improved Time to Market: the ‘off the shelf’ nature of Cloud services and the ability to procure additional capacity rapidly means that the time taken to move from prototype to business deployment can be reduced.
- ‘Green’ Credentials: although large data centres may appear to be intensive consumers of power, it may well prove more efficient to operate a single such installation than the equivalent capacity in individual computers or servers. Furthermore some providers are locating data centres where passive environmental cooling is available.

Many definitions have been promoted, and it is beyond the scope of this paper to review them in detail, but one commonly-cited is that proposed by US analysts Gartner:

“A style of Computing where scalable and elastic IT capabilities are provided as a service to multiple customers using Internet technologies.”<sup>12</sup>

Although not perfect (it, for instance, does not encompass what are termed *private clouds*, where the relevant infrastructure is owned by, or operated for the benefit of, a single large customer<sup>13</sup>) this definition does encapsulate the key attributes that make Cloud computing attractive to customers. By *scalable* Gartner mean that the amount of computing capacity, be it processing or storage,<sup>14</sup> can be varied as required to meet a customer’s requirements; *elastic* indicates that this scaling can be done rapidly in response to changes in demand. This dynamically-adjustable capacity is, as Gartner notes, provided as a service in a manner that is often described as utility-like<sup>15</sup> in terms of being consumed, and frequently paid for, in response to demand.

The final elements of the Gartner definition are that Cloud computing is frequently shared amongst multiple customers and is delivered over the Internet platform. As

---

<sup>12</sup> ‘Experts Define Cloud Computing: Can we get a Little Definition in our definitions?’ [http://blogs.gartner.com/daryl\\_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/](http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/).

<sup>13</sup> A large enterprise might establish its own data centres so as to take advantage of economies of scale and sharing of resources available. The technology and business processes would be very similar to those of Cloud computing, but resources would only be shared within the enterprise. Provided the enterprise is large enough, and with sufficiently diverse business practices (so that demand for resources can be evened out across it) the effect would be the same as migrating its IT infrastructure to the public Cloud, but with the assurance that the enterprise’s data did not go beyond its boundaries.

<sup>14</sup> We make a distinction between processing and storage here in terms of the customer’s perception of the form of computing service that is being purchased. However, it should be noted that for legal purposes, in particular in respect of data protection, all action upon data, be it storage and retrieval or transformation and analysis, is ‘processing’ within the meaning of the Data Protection Directive and associated national legislation.

<sup>15</sup> See, for example, N Carr, “The Big Switch: Rewiring the World, from Edison to Google” (2008), Norton. The term ‘utility’ raises potential regulatory issues that are beyond the scope of this paper.

already noted, these two attributes are not necessarily essential to Cloud computing, although they are common. One of the key attractions of Cloud computing for both customers and providers is that by sharing a pool of computing resources both, indeed sometimes many, parties may benefit financially. A Cloud provider need only provision the total aggregate load of its customer base; this will be less than the maximum load of all its customers in parallel as customers will typically have variable demands that will rarely if ever peak at the same time. Indeed, a customer likely to be particularly attracted to buying computing services from the Cloud would be one with a very variable demand, such that fixed provision via a traditional hosting contract would be wasteful. The provider will thus seek to eliminate the overhead of unused computing capacity; this saving can be passed onto the customer via lower service charges. Providers operating large data centres may well also be able to benefit from economies of scale when purchasing equipment or licences, whilst large data centres, although power-hungry, are likely to be more efficient to cool and operate than an equivalent capacity in terms of stand-alone computers.<sup>16</sup>

In terms of delivery over the Internet, this point relates to another advantage of Cloud computing for both provider and customer: *location independence*. Location independence means, from the customer's perspective, that the services can be accessed from anywhere with suitable communications links. For most services this will indeed be via Internet access, but there is no reason why it could not also be via some other communications infrastructure such as a private corporate network. It is the ubiquity of the service rather than its exact nature that is important. Location independence is also an important factor for providers, who may seek to deploy their infrastructure wherever it is most convenient and efficient, and in a manner that maximises the economies of scale already mentioned. This also means, however, that a customer's data may be stored or processed in one or more locations that are in another country and jurisdiction. The detailed legal implications of such cross-border processing are beyond the scope of this paper and will be addressed in future publications of the QMUL Cloud Legal Project. In this paper, however, we will include examples of provisions in customer agreements whereby Cloud providers make reference to where data will be stored.<sup>17</sup>

---

<sup>16</sup> At 2009 Cloud Computing World Europe, Hakeeret Singh, Head of Data Centre Optimisation for Thomson Reuters, identified four approaches to improving data centre efficiency via Cloud computing. As well as avoiding traditional cooling by building data centres in areas with natural cooling available, and by moving processor load to zones where cooling is cheap ('following the moon') the flexible architecture of Cloud computing allows for hardware redundancy to be reduced. This allows for the resource footprint of data centres both to be reduced and to be scaled alongside the processing demands placed on them.

<sup>17</sup> One practical implication of legal concerns over hosting of data in foreign jurisdictions is that it may encourage providers and customers into agreements by which data is hosted locally; this 'Balkanization of the Cloud' could undermine some of the perceived economic and environmental benefits of Cloud computing by reducing the extent to which data storage and processing could be flexed internationally.

In the course of research for this paper a number of definitions of Cloud computing were examined. Most, although longer than the Gartner definition cited above, broadly described the same 'utility computing' model. Nonetheless it was noted that different definitions placed a differing degree of emphasis on particular aspects of the Cloud computing model. One explanation might be that this is a reflection of the perspective of whoever is producing the definition, which may be based on the nature of their legacy or other business interests. Providers may tend to emphasise the manner in which the Cloud service is delivered (for example, a shared pool of resources) whereas a definition from the viewpoint of customers may instead emphasise the features of the service (for example, scalable resource use and utility-model billing). The authors of this paper have thus proposed a definition that seeks to be neutral in such respects:

- Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly<sup>18</sup> allocated or released in response to demand.
- Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers.
- Charging, where present, is commonly on an access basis, often in proportion to the resources used.

This definition is intended to highlight those aspects of Cloud computing that are central to the concept whilst distinguishing (via qualifiers such as 'typically' or 'generally') those which are common but neither essential nor ubiquitous. It also briefly notes the technology that more than anything else has facilitated the development of Cloud computing: *virtualisation*.

Virtualisation, in the context of Cloud computing,<sup>19</sup> is an extension of the well-established technique by which a computer can emulate another computer and / or operating system. Typically, what is emulated in a cloud environment is a complete virtual instance of a computer, complete with processor, storage, operating system and potentially even an application loaded and ready to run. In effect, this is a 'snapshot' of a real computer running that operating system and application, and will behave as such when run on the computer hosting it. This means that a Cloud computing customer can prepare a virtualised 'image' of a computer, complete with the customer's software,

---

<sup>18</sup> 'Seamless' in this context refers to the manner in which processing or storage capacity is added or removed without any express action from the customer or even awareness by the customer that such adjustment is taking place. In practice, Cloud providers may offer customers the option of explicitly requesting capacity or of allowing it to be varied automatically in response to demand (so-called 'bursting'). ElasticHosts, for example, allows customers to rent specified resources at a particular rate, and optionally to configure bursting to additional resources, this at a higher rate to reflect the less predictable load that ElasticHosts has to supply (<http://www.elastichosts.com/cloud-hosting/pricing>).

<sup>19</sup> Rittinghouse and J Ransome, *Cloud Computing: Implementation, Management and Security* (2010), CRC Press, pp24-28.

which can then be loaded onto a server in the provider's data centre as and when required. This is what permits the rapid scalability of Cloud computing; as the customer's demand varies, the number of virtual instances can be changed accordingly. When a virtual image is deleted from a server, a different one for another customer can be substituted instead. The provider's array of servers comprises the shared pool of computing resources, which are allocated through the medium of customer-specific virtualised images.

Cloud computing services are often characterised in terms of the type of service that is being offered. Common examples include *Infrastructure as a Service* (IaaS), in which a computing resource such as processing power or storage is provided; *Platform as a Service* (PaaS), in which tools for the construction of bespoke applications are provided; and *Software as a Service* (SaaS), in which the service provides functionality akin to an end-user application. This range of services can be viewed as a spectrum of provision from low-level functionality (IaaS) to high-level functionality (SaaS), with PaaS in the middle.<sup>20</sup>

### 3. Classifying Cloud Services and Cloud Provider T&C Documents

For the purposes of this study a 'Provider' is the business organisation that offers the Cloud service, whilst a 'Service' is the particular Cloud service in question. For some providers, such as Adrive, Dropbox or Facebook, the core Cloud service is the provider's only product of substance and the two are essentially congruent; for other providers, the Cloud service may be only one of a number of products, or even a number of Cloud products, that the provider offers. Indeed, some of the providers covered by this survey offered Cloud services that were sufficiently distinct that it was considered worthwhile to analyse the terms and conditions of more than one of them. This survey covers 31 Cloud services offered by 27 discrete providers; we aimed to take as broad a sample as possible of providers offering Cloud services targeted towards the US and European markets.

All the contract terms analysed in this survey were standard terms that were available on the provider's web site for review by potential and current customers. Indeed, as will be noted below, many providers assert that rather than there being an obligation on the provider to notify customers regarding changes to the T&C for a service, customers are required to review the T&C as hosted on the provider website on a regular basis to check whether there have in fact been any changes.<sup>21</sup> The T&C as originally reviewed were downloaded in the first week of January 2010, with a follow-up review of the T&C available in July 2010 for the same services. It is the intention of the QMUL Cloud Legal

<sup>20</sup> The Cloud Computing Use Case Discussion Group of the Open Cloud Manifesto has proposed a detailed taxonomy of Cloud computing services as part of an ongoing study of scenarios for analysing Cloud computing services: "Cloud Computing Use Cases White Paper, Version 4.0", [http://opencloudmanifesto.org/Cloud\\_Computing\\_Use\\_Cases\\_Whitepaper-4\\_0.pdf](http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf).

<sup>21</sup> As will be discussed later in this paper, this may be an onerous task, especially if the provider does not flag up changes to the T&C documents or indicate the date of last change or review.



Project researchers to undertake further reviews of the relevant T&C so as to monitor changes and identify any pattern that may emerge in terms of evolution of T&C.

On the basis of the initial review of T&C described earlier the following broad distinctions were identified and used as the basis of initial categorisation of services:

*Paid/Free*: One of the most obvious distinctions seen in Cloud services is between services for which the customer pays a subscription or usage fee and those which are, at least at first sight, provided for free. Moreover, a number of Cloud providers offer both 'free' and paid versions of products which may differ only slightly. Nonetheless, the distinction between Cloud services that are explicitly charged for and those that are not is generally clear.

*Nature of Service*: As noted in the description of Cloud computing, Cloud services are typically characterised as Software, Platform or Infrastructure 'as a Service', i.e. SaaS, PaaS or IaaS. The services surveyed have thus been classified into one of these categories. As will be apparent from the list of services, the vast majority are categorised as either SaaS or IaaS, with only a handful of PaaS services, Google Apps being the most prominent example. It should be noted though that some 'online storage' services, such as ADrive or Dropbox, may appear to be IaaS but in fact are more accurately described as storage-related SaaS, in that they package an infrastructure resource and present it as, in effect, a backup or file-sharing application.

*Type of Customer*: For the purpose of this analysis we consider customers to be in three broad classes: Consumers, Small/Medium Enterprises (SME) and Corporate / Public Administration. Some Cloud services, such as Apple's MobileMe, are marketed primarily to a consumer customer base, although this does not preclude their use for business purposes, including by larger organizations. This is also true of Cloud services that exist primarily for hosting user-generated content, such as Facebook; again though, such social networking services may also be used by organisations for publicity purposes.<sup>22</sup> At the other end of the market, services such as those offered by Salesforce and Iron Mountain are very much directed at large organizations, be they corporate or public-sector. This division appears to be most distinct at the application end of the Cloud spectrum; it stands to reason that applications will be tailored to specific markets. Infrastructure services are less clearly stratified in terms of the target customer base; one of the providers surveyed (GoGrid) states that its service is for business, rather than consumer, use, but a number of others indicate that they will accept payment by credit card and have no stipulation against consumer use. Indeed, in view of one of the central attributes of Cloud computing, the elasticity of resources, it is in principle just as easy for a provider to sell a time unit on a single processing or storage instance as it is to sell that instance as an incremental resource increase to a large existing customer. The use of standard-form contract terms and 'click-through' ordering means that a provider may have no more administrative overhead in setting up a contract with an individual

<sup>22</sup> For example YouTube is primarily a personal video sharing service, but the BBC uses it to showcase extracts from its programming. 'BBC and YouTube partner to bring short-form BBC content to online audiences',

[http://www.bbc.co.uk/pressoffice/pressreleases/stories/2007/03\\_march/02/you\\_tube.shtml](http://www.bbc.co.uk/pressoffice/pressreleases/stories/2007/03_march/02/you_tube.shtml).

customer than with a large organization, so may be equally willing to offer Cloud services to both.

In terms of the nature of service and type of customer it is therefore possible to propose a 'service category matrix' in which services are mapped against both these aspects (Figure 1).

**Figure 1 - Cloud Service Category Matrix**

		Applications, Utilities and Services	Development Platform	Computing Infrastructure
Corporate/ Public Administration	Corporate/ Public Administration			
	SME			
	Personal			

The spectrum of service types runs from left to right, from SaaS through PaaS to IaaS. The target customer market runs from bottom to top, from those services aimed principally at private consumers through those aimed at small and medium enterprises (SME) to those marketed at large organisations such as corporations or government agencies.

It is important to note that these are not firm boundaries, especially in terms of target customers. Whilst some Cloud services are squarely aimed at either personal or corporate customers, others will be directed at a wider range. For example, services that provide document processing and hosting may be targeted both at consumers and SMEs, whilst services for human resources management may be intended for use by organisations of all sizes, from SMEs to large corporations or even branches of government.

Table 1 lists the Cloud services covered by this survey together with a broad description of the type of service offered and the market that the service is aimed at. This last criterion is necessarily a subjective assessment, as there is no clear boundary between different types of Cloud service (for instance, storage may be offered as a dedicated service in its own right or as an element of virtualised server provision) nor between different target market segments. Furthermore, as noted earlier, few providers explicitly market their services to a particular audience. Nonetheless, on undertaking a survey of providers it was evident that there were differences in the way that services were being marketed and the classification below reflects the authors' best endeavour to interpret this.

**Table 1 – Cloud Providers covered by Survey**

Provider	Service	Type of Service	Target Market
37signals	Basecamp <sup>23</sup>	Collaborative project management tool	SME / Corporate
3tera	AppLogic <sup>24</sup>	Virtualised application hosting via IaaS	SME / Corporate
Adrive	Adrive <sup>25</sup>	File hosting and backup via SaaS	Personal / SME
Akamai	Hosting <sup>26</sup>	Web acceleration via IaaS distributed caching	Corporate
Amazon	Amazon Web Services <sup>27</sup>	Virtualised application hosting and data storage via IaaS	SME / Corporate
Apple	iWork.com <sup>28</sup>	Collaborative document review via SaaS	Personal

<sup>23</sup> Service description at <http://basecamphq.com/index2> and T&C at <http://basecamphq.com/terms>.

<sup>24</sup> Service description at <http://www.3tera.com/AppLogic/> and T&C at <http://www.3tera.com/Terms/index.php>.

<sup>25</sup> Service description at <http://www.adrive.com/> and T&C at <http://www.adrive.com/terms>.

<sup>26</sup> Service description at <http://www.akamai.com/html/solutions/index.html> and T&C at [http://www.akamai.com/dl/akamai/Akamai\\_Terms\\_Conditions\\_2009.pdf](http://www.akamai.com/dl/akamai/Akamai_Terms_Conditions_2009.pdf) and <http://www.akamai.com/html/policies/index.html>.

<sup>27</sup> Service description at <http://aws.amazon.com/> and T&C at <http://aws.amazon.com/terms/>.

<sup>28</sup> Service description at <http://www.apple.com/uk/iwork/iwork-dot-com/> and T&C at <http://www.apple.com/legal/iworkcom/en/terms.html> and <http://www.apple.com/legal/privacy/>.

Provider	Service	Type of Service	Target Market
Apple	MobileMe <sup>29</sup>	Email, file hosting and personal information management via SaaS	Personal
Decho	MozyHome / Mozypro <sup>30</sup>	File hosting and backup via SaaS	Personal / SME
Dropbox	Dropbox <sup>31</sup>	File hosting and backup via SaaS	Personal / SME
ElasticHosts	ElasticHosts Cloud <sup>32</sup>	Application hosting via IaaS	SME
Facebook	Facebook <sup>33</sup>	Social networking (including application sharing) via SaaS	Personal
Flexiant (formerly Xcalibre)	FlexiScale <sup>34</sup>	Application hosting via IaaS	SME
G.ho.st	G.ho.st ( <b>closed</b> ) <sup>35</sup>	Former virtualised desktop via SaaS	Personal
GoGrid	GoGrid <sup>36</sup>	Virtualised application hosting and data storage via IaaS	SME / Corporate

<sup>29</sup> Service description at <http://www.apple.com/uk/mobileme/> and T&C at <http://www.apple.com/legal/mobileme/en/terms.html> and <http://www.apple.com/legal/privacy/>.

<sup>30</sup> Service description at <http://mozy.com/products> and T&C at <http://mozy.com/terms>.

<sup>31</sup> Service description at <https://www.dropbox.com/features> and T&C at <https://www.dropbox.com/terms>.

<sup>32</sup> Service description at <http://www.elastichosts.com/> and T&C at <http://www.elastichosts.com/cloud-hosting/terms-of-service>.

<sup>33</sup> Service description at <http://www.facebook.com/help/> and T&C at <http://www.facebook.com/terms.php> and <http://www.facebook.com/policy.php>.

<sup>34</sup> Service description at <http://www.flexiant.com/> and T&C at <http://www.flexiant.com/products/flexiscale/terms/>.

<sup>35</sup> Service description (archived) at <http://web.archive.org/web/20080616200715/http://www.g.ho.st/> and T&C (archived) at <http://web.archive.org/web/20080511011825/www.g.ho.st/TermsOfService.html>.

<sup>36</sup> Service description at <http://www.gogrid.com/cloud-hosting/> and T&C at <http://www.gogrid.com/legal/terms-service.php>.

Provider	Service	Type of Service	Target Market
Google	Google Apps Premier <sup>37</sup>	Application creation and hosting via PaaS	SME / Corporate
Google	Google Docs <sup>38</sup>	Document creation and sharing via SaaS	Personal / SME
IBM	Smart Business Cloud <sup>39</sup>	Virtualised application hosting and data storage via IaaS	SME / Corporate
Iron Mountain	LiveVault <sup>40</sup>	Data archiving via SaaS	Corporate
Joyent	Joyent Cloud <sup>41</sup>	Application hosting via IaaS	SME/Corporate
Microsoft	.Net <sup>42</sup>	Application development and hosting via PaaS/IaaS	SME/Corporate
Microsoft	Live Mesh <sup>43</sup>	Data sharing and sync via SaaS	Personal
Microsoft	SQL Azure Database <sup>44</sup>	Data storage and search via IaaS	SME/Corporate
Nirvanix	Storage Delivery Network <sup>45</sup>	Data storage via IaaS	SME/Corporate

<sup>37</sup> Service description at <http://www.google.com/apps/intl/en-GB/business/index.html> and T&C at [http://www.google.com/apps/intl/en-GB/terms/premier\\_terms\\_ie.html](http://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html).

<sup>38</sup> Service description at <http://www.google.com/google-d-s/intl/en/tour1.html> and T&C at <http://www.google.com/accounts/TOS>.

<sup>39</sup> Service description at [http://www.ibm.com/ibm/cloud/smart\\_business/](http://www.ibm.com/ibm/cloud/smart_business/) and T&C at <https://www-180.ibm.com/cloud/enterprise/beta/static/Z125-8338-01-30Sept09CloudServicesAgreementInternational.pdf>.

<sup>40</sup> Service description at <http://www.ironmountain.com/digital/server/> and T&C at <http://ironmountain.com/legal/livevaultc.asp>.

<sup>41</sup> Service description at <http://www.joyent.com/services/> and T&C at <http://www.joyent.com/about/policies/terms-of-service/>.

<sup>42</sup> Service description at <http://www.microsoft.com/net/overview.aspx> - T&C not available online.

<sup>43</sup> Service description at <https://www.mesh.com/Welcome/overview/overview.aspx> and T&C at <http://explore.live.com/microsoft-service-agreement?mkt=en-GB>.

<sup>44</sup> Service description at <http://www.microsoft.com/windowsazure/sqlazure/> - T&C not available online.

Provider	Service	Type of Service	Target Market
PayPal	PayPal Merchant Services <sup>46</sup>	Payment and accounts handling via SaaS	Personal/SME
Rackspace UK	Rackspace Cloud <sup>47</sup>	Virtualised application hosting and data storage via IaaS	SME / Corporate
Salesforce	Salesforce CRM <sup>48</sup>	HR and CRM services via SaaS	SME/Corporate
Symantec	Norton Online <sup>49</sup>	Backup via SaaS	Personal
The Planet	General (inc Storage Cloud) <sup>50</sup>	Virtualised application hosting and data storage via IaaS	SME / Corporate
UKFast	CloudHosts <sup>51</sup>	Application hosting via IaaS	SME/Corporate
Zecter	ZumoDrive <sup>52</sup>	File hosting and backup via SaaS	Personal / SME
ZoHo	Zoho Services <sup>53</sup>	Document creation and sharing via SaaS	Personal / SME

<sup>45</sup> Service description at <http://www.nirvanix.com/products-services/storage-delivery-network/index.aspx> and T&C at <http://www.nirvanix.com/how-to-buy/terms.aspx>.

<sup>46</sup> Service description at <https://www.paypal-business.co.uk/> and T&C at [https://cms.paypal.com/cms\\_content/GB/en\\_GB/files/ua/ua.pdf](https://cms.paypal.com/cms_content/GB/en_GB/files/ua/ua.pdf).

<sup>47</sup> Service description at <http://www.rackspace.co.uk/cloud-hosting/> and T&C at <http://www.rackspace.co.uk/rackspace-home/legal/general-terms/>.

<sup>48</sup> Service description at <https://www.salesforce.com/crm/products.jsp> and T&C at <https://www.salesforce.com/company/msa.jsp>.

<sup>49</sup> Service description at <http://www.symantec.com/en/uk/norton/online-backup> and T&C at [http://www.symantec.com/content/en/us/about/media/NOBU\\_TOS\\_21\\_USE.pdf](http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf).

<sup>50</sup> Service description at <https://www.theplanet.com/servers/beta.aspx> and T&C at <http://content.theplanet.com/Documents/legal/Planet-TOS.pdf>.

<sup>51</sup> Service description at <http://www.ukfast.co.uk/cloudhosts.html> and T&C at <http://www.ukfast.co.uk/terms.html>.

<sup>52</sup> Service description at <http://www.zumodrive.com/tour> and T&C at <http://www.zumodrive.com/tos>.

<sup>53</sup> Service description at <http://www.zoho.com/index.html> and T&C at <http://www.zoho.com/terms.html>.

In this paper we use the T&C to refer to the document, or more usually set of documents, containing the terms governing the relationship between the customer and the Cloud service provider. T&C documents came in a number of forms, from relatively short and simple, to lengthy, complex and split over several documents, but generally include the following:

**Terms of Service (ToS).** This document details the overall relationship between the customer and provider. It usually contains the commercial terms if the service is paid for, and includes legal clauses such as choice of law and disclaimers. If there are other T&C documents it typically incorporates them by reference.

**Service Level Agreement (SLA).** This document specifies the level of service the provider aims to deliver together with the process for compensating customers if the actual service falls short of that. Accordingly, SLAs are associated only with paid-for services.

**Acceptable Use Policy (AUP).** This document details the permitted (or in practice, forbidden) uses of the service.

**Privacy Policy.** This document describes the provider's approach to using and protecting the customer's personal information. Although usually termed a 'Privacy policy' it often incorporates terms specifically relating to data protection.

Although some providers do present all four T&C documents it is quite common to see the AUP folded into the ToS, whilst many services – even some paid ones – do not offer an SLA. However, a separate privacy policy is usually made available; this may be because the provider has a single privacy policy applying to all its online services rather than just Cloud provision and may also reflect the fact that privacy policies tend to address compliance rather than contractual issues. Where separate T&C documents are presented, one will typically incorporate the others by reference.<sup>54</sup>

This analysis is based on the full range of T&C documents issued by the surveyed providers. We noted that even where there are separate documents comprising the T&C specific terms are not always allocated as neatly as the above definitions might suggest. In particular, we noted several instances where terms relating to privacy were found in the ToS or AUP as well as the Privacy Policy.

---

<sup>54</sup> For example, the ToS for ThePlanet states the following: *“These Terms of Service hereby incorporate by reference the SLA, The Planet’s Acceptable Usage Policy (as in effect from time to time as set forth on The Planet’s website, the “AUP”) and the Order Form each of which is made a part of these Terms of Service and collectively referred to herein as the “Agreement.” Customer’s use of The Planet’s website, The Planet Network, and the Products and Services is also subject to Customer’s acceptance and compliance with these Terms of Service, the AUP, the SLA and the Order Form. Capitalized terms used herein without being defined herein shall have the meaning ascribed to such capitalized term in the SLA or AUP, as applicable.”* (See note 50.)

One important point to note is that several large providers have more than one set of T&C documents for a given service. Depending on location, a customer may be offered T&C tailored to the appropriate local laws. Such localisation was seen in relation to services from major providers such as Microsoft and Google. Other providers, such as IBM, were seen to offer T&C that included a range of optional elements that applied depending upon the location of the customer.<sup>55</sup>

## 4. Categorising and Analysing Terms

Initial review of the T&C documents covered in this project indicated that although they vary considerably in content and length there are many features that commonly appear. We have identified in particular 20 types of term that are either common or, if rare, are of sufficient interest to our analysis to merit specific note when they are seen.

### 4.1. Contract

The general basis on which providers and customers enter into a relationship falls into two clear categories, depending on whether the provider is offering a paid service or a free one. However, this distinction is not a clear one. For instance, some 'free' services may impose non-monetary costs on the customer, such as contextual advertising or the imposition of licence terms that allow the provider to re-use the customer's data for its own purposes.<sup>56</sup> Equally, paid services themselves fall into a spectrum between those entered into on the basis of the standard-form contract of the provider and those where the contract terms are fully negotiated, depending on the relative bargaining power of provider and customer.<sup>57</sup> Furthermore, some services may offer a free trial period conditional on the customer giving payment details, which then converts into a paid contract; such a service is classed as 'paid' for the purposes of this analysis.

Nonetheless, one can observe a distinction between the T&C of Cloud services that are offered as a paid utility service and those provided on an at least notionally free or low-cost, flat-rate basis. The former typically include IaaS infrastructure provision, as exemplified by Amazon Web Services EC2 and S3 products. The latter are typically directed at consumers and offer services such as email, file storage or content hosting. Many social networking sites, such as Facebook, also offer the capacity to run applications and host user content (for example, photographs) and so are deemed to be consumer-oriented Cloud services for the purposes of this analysis.

For paid services, T&C typically specify the initial duration of the contract, its renewal period and payment structure, and the steps to be taken by either party to terminate the contract. It is not unusual to see a provision that the contract will continue indefinitely until it is terminated. For example, Amazon AWS's T&C provide that:

---

<sup>55</sup> See sections 4.2 (Choice of Law) and 4.17 (Limit of Liability) for examples.

<sup>56</sup> See further section 4.12.

<sup>57</sup> As explained in the introduction, this paper concentrates on standard-form contracts for Cloud computing services.



*“The Agreement will remain in effect until terminated by you or us in accordance with this Section 3.”*<sup>58</sup>

Contracts for paid service typically include clauses defining breaches by the customer that will result either in managed termination of the contract (for example, after one payment period in default) or immediate termination for cause. The most common justification specified for immediate termination is a serious breach by the customer of the provider’s AUP (as discussed further below).

For free services there is no periodic payment structure and thus no fixed contract term.<sup>59</sup> Nonetheless, the provider will generally specify the means by which it can bring the relationship to an end so as to avoid indefinite obligations to host customer data. One of these, as with paid contracts, will often be a breach of the AUP (for example, 37Signals, ADrive and Google Docs). Another will typically be an ‘inactive account’ clause by which a provider can excuse itself from supporting accounts that are not being paid for (being free) but which are not being used. Dropbox, for instance, reserves the right to close accounts that are not accessed for 90 days.<sup>60</sup>

This paper does not seek to make a detailed analysis of the enforceability of specific terms; a review of contracting and consumer protection will form the subject of a future paper within the QMUL Cloud Legal Project. However, it should be noted that consumers are likely in European legal systems to gain the benefit of laws shielding them against unfair or unreasonable terms. Businesses typically receive a lesser degree of protection, although it is still the case that particularly harsh terms may be deemed unenforceable.<sup>61</sup>

---

<sup>58</sup> See note 27.

<sup>59</sup> Indeed, under some models of contract formation it may be questionable whether an enforceable contract exists between the provider and customer. Under English law, for example, the customer may be held not to have provided any consideration, although it could be held that the customer has acted to his or her detriment in some other manner (for example, permitting commercial use to be made of personal data, or agreeing to abide by terms such as exclusion clauses) that forms valid consideration. However, even if the agreement between the provider and customer does not form a valid contract, it may well comprise a conditional licence by which the provider offers a free service in return for the customer abiding by the provider’s terms. As such, for the purposes of this analysis it will be assumed that the T&C for the service are valid and enforceable to the extent local law permits, be it under contract or (for the provider) as the terms of a conditional licence.

<sup>60</sup> *“Dropbox reserves the right to terminate Free Accounts at any time, with or without notice. Without limiting the generality of the foregoing, and without further notice, Dropbox may choose to delete and/or reduce: (i) any or all of Your Files if your Free Account is inactive for 90 days; and (ii) previous versions and/or prior backups of Your Files.”* (See note 31.)

<sup>61</sup> It should not be assumed that Small and Medium Enterprises (SMEs) are devoid of protection from unfair terms. In *Kingsway Hall Hotel v Red Sky IT (Houslow)* [2010] EWHC 965 (TCC) HHJ Toulmin held that elements of an IT services contract between a non-specialist business customer and a specialist provider contracting on its standard terms could, despite it being a business-to-business agreement, be held to be unfair and unenforceable. Although this case did

#### 4.2. *Applicable Law*

The majority – although by no means all – of the T&C surveyed include terms that assert that the contract is covered by the laws of a specific jurisdiction. This is typically the jurisdiction in which the provider has its principal place of business, but in the case of some providers (typically ones with international operations) the T&C may specify that differing legal systems apply depending on the location of the customer.

Of the 31 T&C analysed, the breakdown of choice of law is as listed in Table 2. Note that where T&C mandate arbitration in a particular jurisdiction, it has been assumed that the local law of that jurisdiction applies.

**Table 2 – Breakdown of Choice of Law**

<b>Choice of Law</b>	<b>Number</b>
The law of a particular US state. This is most commonly California, but also includes Massachusetts (Akamai), Washington (Amazon), Utah (Decho) and Texas (The Planet).	15
English law, probably because it is the law of the jurisdiction in which the service provider is based.	4
English law, for customers in Europe or the EMEA.	4
The law of other EU jurisdictions for European customers (for example, Irish law for Apple, Luxembourg law for some Microsoft services).	2
Scottish law (Flexiant).	1
The customer's local law.	2
No choice of law expressed or implied, or an ambiguous choice given (for example, 'UK Law' for g.ho.st).	3

It should be noted that for the purposes of this analysis the T&C obtained were those that would be offered to a prospective customer in England. Some of the larger providers offer T&C tailored to customers in England / the UK, Europe or the EMEA area. The survey showed that for the set of providers examined a customer in England would be offered a contract governed by English law in 10 of 31 cases: in 4 because the provider operates under English law; in 4 because the provider selects English law as a regional choice; and 2 because the provider adopts local law. For the other cases, the customer would be offered a contract governed by Scottish law, other European law (Irish or Luxembourg law) or the law of one of 5 different US states. In some, the

---

not involve a Cloud service contract the terms in question were typical of those found when surveying the T&C of Cloud providers.

customer would not be offered a valid choice of law at all.<sup>62</sup> It should be noted that choice-of-law terms may be more significant for corporate or SME customers, since, as noted above, individual consumers may, depending on the applicable law, be shielded by consumer protection laws from contract terms that purport to impose a foreign legal system. A large corporate customer would presumably seek to tailor a cloud contract to ensure that it was not subject to a legal system the customer felt inappropriate; while for government customers, or other public-sector bodies, subjecting themselves to a foreign law will often be completely unacceptable.

### **4.3. Jurisdiction**

The position with choice of forum for settling disputes between the provider and customer is very similar to that with choice of law. Not surprisingly (as it would be of questionable wisdom for a provider to seek to do otherwise) providers generally specify a jurisdiction compatible with the specified legal system. In many cases, especially where the law of a particular US state is asserted, the provider will include a term stating that claims against it must be brought in the courts of a particular city within that state. For instance, Symantec requires that claims be brought in the courts of Santa Clara; this is a provision which may bear heavily on customers who take advantage of the international nature of Cloud computing services, although it may of course not be enforceable against consumers, depending on local consumer protection law.<sup>63</sup>

In addition to asserting jurisdiction, a number of providers seek to impose relatively short limitation periods within which a customer must bring a claim in respect of the service. IBM and Rackspace require claims to be brought within 2 years; Apple, within one year; and ADrive, within 6 months.<sup>64</sup> Again, such terms may well not be enforceable, particularly against European consumers.<sup>65</sup>

### **4.4. Arbitration**

A Cloud computing service contract, in common with many other sorts of commercial contract, may give the option of commercial arbitration as an alternative to litigation or may even seek to require it. Although common in business-to-business contracts, such

---

<sup>62</sup> In such cases a European court would apply the 'Rome I' Regulations to determine the applicable law (Regulation (EC) 593/2008 on the law applicable to contractual obligations, OJ L177/6, 4.7.2008). For a consumer customer, Art. 6 of these Regulations would generally apply the law of the consumer's domicile.

<sup>63</sup> Similar considerations as to enforceability, especially against individual consumer customers, apply as for choice of law, including the points made at note 61.

<sup>64</sup> *"Regardless of any statute or law to the contrary, any claim, cause of action, or demand for arbitration against ADrive arising out of or related to this Agreement or use of ADrive's services must be filed within six months of the date upon which You were or should have first been aware of the existence of the grounds for Your claim or cause of action."* (See note 25.)

<sup>65</sup> See sub-paragraph (q) of the Annex to Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts.

terms may be deemed to impose unfair constraints upon a consumer's ability to seek a remedy.<sup>66</sup>

Seven of the 31 T&C analysed include some form of clause seeking to impose arbitration. Three providers (ADrive, Nirvanix and Zoho) require customer disputes to be resolved through arbitration in all cases, whilst 3Tera does so for claims valued at over US\$500. IBM, Iron Mountain and Microsoft (for LiveMesh) all have terms that impose arbitration on customers in some countries but not others. IBM, for its Smart Business Cloud, mandates arbitration for disputes arising in the People's Republic of China, South-East Asian states, and states within Eastern Europe or the Former Soviet Union. Such terms are likely to reflect a lack of familiarity with, or confidence in the effectiveness of, the judicial systems in such countries. Where such clauses apply they generally stipulate a forum for arbitration and a recognised arbitration body; Nirvanix, for instance, asserts the rules of the American Arbitration Association:

*“Any dispute relating in any way to your use of Nirvanix Properties will be submitted to confidential arbitration in San Diego, California ... Arbitration under this Agreement will be conducted under the rules then prevailing of the American Arbitration Association. The arbitrator's award will be binding and may be entered as a judgment in any court of competent jurisdiction.”*<sup>67</sup>

#### **4.5. Acceptable Use**

If there is one area of Cloud provider T&C in which they are superficially most varied yet are in fact substantially alike it is in respect of the rules they impose on the manner in which customers may use (and, more specifically, may not abuse) the service. Such rules, which are often presented in a separate AUP, are present in some form in every one of the T&C analysed and reflect the providers desire to shield themselves from liability arising out of the conduct of their customers.<sup>68</sup> At first sight they vary in their extent and detail, from brief injunctions against illegal conduct to extremely broad

---

<sup>66</sup> For example, terms seeking to impose compulsory arbitration against consumer customers within the UK are highlighted as being potentially unfair under the UTCC Directive (see note 65 above). While in the US, such clauses have been held to be valid, see *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997).

<sup>67</sup> See note 45.

<sup>68</sup> The English courts have recently held the extent to which hosts have sought to control the illicit behaviour of users to be very relevant in determining their liability for such misconduct. In *L'Oréal SA v eBay International AG* [2009] R.P.C. 21 eBay escaped joint liability for trade mark infringements because of its proactive efforts to restrain such behaviour by users; by contrast, in *Twentieth Century Fox Film Corp v Newzbin Ltd* [2010] E.C.C. 13 Newzbin was held liable for copyright infringement owing to its failure to prevent (and indeed its tacit encouragement of) illicit file-sharing by its users. (R. Massey, 'Case Comment: *Twentieth Century Fox Film Corporation v Newzbin Ltd*', C.T.L.R. 2010, 16(6), 164-166.)

ranging and detailed lists of prohibited behaviour, but on careful examination they prove to be very similar in their scope and effect.

The vast majority of Acceptable Use terms prohibit a consistent set of activities that providers consider to be improper or outright illegal uses of their service. These include bulk unsolicited commercial email ('spam'), fraud, gambling, hacking into other systems or the hosting of content that is obscene, defamatory or such as to promote discrimination or incite hatred. In many cases, the difference between shorter and longer AUPs is the level of detail with which such activities are described. A good example of a short AUP is that imposed by ZoHoServices:

*"You agree to be solely responsible for the contents of your transmissions through the Services. You agree not to use the Services for illegal purposes or for the transmission of material that is unlawful, defamatory, harassing, libellous, invasive of another's privacy, abusive, threatening, harmful, vulgar, pornographic, obscene, or is otherwise objectionable, offends religious sentiments, promotes racism, contains viruses, or that which infringes or may infringe intellectual property or other rights of another. You agree not to use the Services for the transmission of "junk mail", "spam", "chain letters", "phishing" or unsolicited mass distribution of email. We reserve the right to terminate your access to the Services if there are reasonable grounds to believe that you have used the Services for any illegal or unauthorized activity."*<sup>69</sup>

Although other providers' AUPs may be much more extensive and detailed than this, they tend on examination to prohibit very much the same forms of behaviour and misuse.

A number of providers do, however, go further than this in setting out examples of unacceptable activity. Some, such as ElasticHosts, prohibit the use of their service for 'safety-critical' applications where the failure of the service may result in injury or loss of life. Others, such as Rackspace, have terms prohibiting some quite unusual activities, such as any use in connection with the design of weapons of mass destruction! In a similar vein, several US-based providers such as ADrive do not permit their services to be used by, or to host material for, nationals of a list of nations including Cuba, Iran and North Korea.<sup>70</sup>

Some providers have exclusions that appear to reflect their target market. Iron Mountain, which offers a service specifically tailored to business data backup, prohibits use of its Cloud for other purposes, whilst Facebook prohibits anyone who is a convicted sex offender from using the service.

In summary, the AUP for the providers covered by this survey appear on first examination to vary considerably. On closer examination, it is clear that they prohibit the

---

<sup>69</sup> See note 53.

<sup>70</sup> I.e. countries subject to embargoes and economic sanctions imposed by US law and enforced by the US Office of Foreign Assets Control.

same types of behaviours with a high degree of consistency. It should be noted though that this survey is of providers in the US and European markets, where there is likely to be a more or less common 'western' set of cultural and legal assumptions about what constitutes 'acceptable' behaviour.

#### **4.6. Variation of Contract Terms**

An area where significant divergence is seen between T&C is in the provision they make for variation of their own terms. Eight of the surveyed providers make no mention of any variation process, but the remainder reserve the right to do this. Even among those, however, the procedure for doing so varies considerably. Thirteen of these providers incorporate a term that states that they may amend their T&C simply by posting an updated version on their website, and that continued use of the service by the customer is deemed as acceptance of the new T&C. A typical example of such a term is that found in Zecter's T&C for ZumoDrive:

*"[Zecter] reserves the right to update and change the Terms of Service from time to time without notice. Any new features that augment or enhance the current Service, including the release of new tools and resources, will be subject to the Terms of Service. Continued use of the Service after any such changes will constitute your consent to such changes. You can review the most current version of the Terms of Service at any time at: <http://www.zumodrive.com/tos>"*<sup>71</sup>

Where the services are provided under a paid contract, such a term will typically include reference to a break clause by which a customer who does not wish to accept the amended T&C may withdraw from the agreement.

Apple reserves the right to amend its T&C but states that it will inform customers by email. Only three (Google Apps Premier, Iron Mountain and Salesforce CRM) state that changes to the T&C may only be in writing with the agreement of both parties. Some, such as UKFast, simply state that they may vary their T&C, with no further note on whether the customer will be notified of this or what constitutes acceptance of the change.

#### **4.7. Data Integrity**

A natural concern for Cloud computing customers is that data placed into the provider's Cloud be secure against loss, be it loss of integrity or availability (resulting, for example, from corruption or deletion) or loss of confidentiality (due perhaps to a security breach or an unauthorised disclosure). Our survey found however that most providers not only avoided giving undertakings in respect of data integrity but actually disclaimed liability for it.

The majority of providers surveyed expressly include terms in their T&C making it clear that ultimate responsibility for preserving the confidentiality and integrity of the

---

<sup>71</sup> See note 52.

customer's data lies with the customer. A number (for example, Amazon, GoGrid, Microsoft) assert that they will make 'best efforts' to preserve such data, but nonetheless include such a disclaimer. A number of providers go so far as to recommend that the customer encrypt data stored in the provider's Cloud (for example, GoGrid, Microsoft) or specifically place responsibility on the customer to make separate backup arrangements:

*"You bear sole responsibility for any and all data used in connection with the development, operation or maintenance of any software programs or services that you use in connection with your access to or use of the Services, including without limitation taking the steps necessary to back up such data, software programs or services."* (Microsoft .Net)

Amazon's T&C for Amazon Web Services also exemplify this approach:

*"...you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications."*<sup>72</sup>

Significantly, such terms are imposed by storage providers such as ADrive and Apple for services that for many (especially individual) customers will be their 'separate backup arrangement'. In effect, a number of providers of consumer-oriented Cloud services appear to disclaim the specific fitness of their services for the purpose(s) for which many customers will have specifically signed up to use them.<sup>73</sup> Some providers (for example, Rackspace) state that data integrity will only be guaranteed where the customer has paid for additional specific backup services.

A small number of the providers surveyed give more positive assurances. For example, Salesforce CRM's T&C state that appropriate measures will be taken to safeguard customer data. It is interesting to note that two providers offering specific backup services, Symantec and Iron Mountain, make no mention of data integrity in their T&C. It may well be that both providers assume it to be implicit from the nature of their service that they will assure such protection and so see no need to provide for it expressly. However, as noted above, other providers offering storage and backup services specifically disclaim such representations. The distinction tends to be between those services that provide backup facilities for no fee, where there is no assurance, and those which charge for such facilities, where there is.

---

<sup>72</sup> See note 27.

<sup>73</sup> An alternative, and perhaps more charitable interpretation, is that such terms encourage customers not to rely on what may prove to be a single point of failure.

#### 4.8. Data Preservation

An important issue for many customers is what will happen to their data after the relationship with the provider comes to an end. In fact, there are two issues here: whether there will be any opportunity for the customer to gain access to the data (for example, to retrieve it for use elsewhere) once the contract has ended, and whether there is assurance from the provider that data will effectively be deleted after this stage. The former point is likely to be significant for many customers because they are likely to want assurance that data put into the Cloud may be recovered in a managed fashion. The significance of the latter point is likely to be that customers will be concerned as to whether data they entrust to a Cloud service provider will ever be deleted comprehensively from the Cloud. CNN has published an animated video that highlights the replication and persistence of customer data as benefits of the Cloud,<sup>74</sup> but the converse of that argument is the concern that data, once uploaded and copied in this manner, may never be truly expunged from the Cloud. Were this perception to become widespread, it could become a significant barrier to the large-scale take-up of such services.

Most of the providers surveyed fall into three broad camps in respect of the way in which they state that they will deal with customer information following the end of the relationship between them and the customer.

The first set of providers asserts that they will normally preserve customer data for a set period of time following the end of a service contract. Amazon, ElasticHosts and Zecter all stipulate 30 days (or one month) as the grace period during which a former customer may access data. However, this grace period may not apply if the contract was terminated for cause, such as breach of the relevant AUP. Other providers offer shorter grace periods: Nirvanix 15 days, and Decho only 3. Furthermore, access during the grace period may itself be subject to charges and other conditions; for example, Amazon AWS's T&C include the following term:

*“In the event of any termination by us of any Service or any set of Services, or termination of this Agreement in its entirety, other than a for cause termination under Section 3.4.1, (i) we will not take any action to intentionally erase any of your data stored on the Services for a period of thirty (30) days after the effective date of termination; and (ii) your post termination retrieval of data stored on the Services will be conditioned on your payment of Service data storage charges for the period following termination, payment in full of any other amounts due us, and your compliance with terms and conditions we may establish with respect to such data retrieval.”*<sup>75</sup>

<sup>74</sup> <http://www.cnn.com/2009/TECH/11/04/cloud.computing.hunt/index.html>. The article that accompanies this video may be criticised for a lack of precision, but given the reach of publishers like CNN such ‘popular’ explanations of cloud computing may be significant in shaping perceptions of the cloud.

<sup>75</sup> See note 27.



The T&C go on to note, however, that:

*“Except as provided in Sections 3.7.1 and 3.7.2 above, we shall have no obligation to continue to store your data during any period of suspension or termination or to permit you to retrieve the same.”*<sup>76</sup>

The references to the other sections are for termination due to non-payment and for suspension, as distinct from termination for cause. The effect of this clause is thus for Amazon to assert that, where the service is terminated in other circumstances, including but not limited to termination for cause, it is under no obligation to preserve customer data.

The second set of providers asserts that customer data will be deleted immediately the relationship between customer and provider ends. In this respect it is notable that Apple takes such an approach for its MobileMe product, even though this is a paid service:

*“Upon termination of your account you lose all access to the Service and any portions thereof, including, but not limited to, your Member Account (any Sub-accounts thereunder), Subscriber ID, email account, iDisk, domains, iChat account and MobileMe Gallery albums. In addition, Apple shall delete all information and data stored in or as a part of your account(s) including, but not limited to, data files, email, albums and preferences.”*<sup>77</sup>

Such terms raise the question of the provider’s position should a court later decide that termination of the contract was ineffective. The provider could be in breach of contract, or of a potential duty in bailment<sup>78</sup> to preserve the customer’s data. Indeed, it might even be liable to criminal prosecution for offences regarding the unauthorised deletion of data.<sup>79</sup>

The third set takes a hybrid approach, with providers stating that they will be under no obligation to preserve data after the end of the relationship, but not undertaking to delete data or noting that a grace period may apply at their discretion. Flexiant, for example, says that customer data access will be at its discretion, whilst Google, for its Google Docs service, states that customer data may be deleted at any time. Microsoft disclaims any obligation to preserve customer data post-termination (.Net and Live Mesh) or requires the removal of data by Customers on termination (SQL Azure Database):

*“Upon the expiration of the term or any termination or cancellation of this agreement, your rights to access or use the Services immediately cease, and you must promptly remove from the Services any data, software programs or services (if any) used in connection with your access to or use of the Services. If*

---

<sup>76</sup> *ibid.*

<sup>77</sup> See note 29.

<sup>78</sup> See note 107 for a reference to a discussion of bailment in the context of data stored by a Cloud provider.

<sup>79</sup> E.g., UK Computer Misuse Act 1990, s. 3

*you do not remove such data, software programs or services from the Services, we reserve the right to remove them in accordance with our normal business practices for the Services.” (Microsoft .Net)*

*“Upon termination or cancellation of the service by you or us for any reason, Microsoft may delete your data permanently from our servers. You are responsible for taking all necessary steps to back up your data and ensuring that you maintain your primary means of business.” (Microsoft LiveMesh)<sup>80</sup>*

*“Upon cancellation, suspension or any termination, your right to use the Services stops right away and you must immediately remove your Data and applications from the Services. You are responsible for taking the steps necessary to back up your Data. Upon any termination of this agreement, all other rights granted to you by this agreement will also automatically terminate.” (Microsoft SQL Azure Database)*

Some ‘free’ providers, offering storage to private customers, may not have a specific contract period. As such they may state that they will delete data in apparently dormant accounts. An example is Zoho, which defines delinquency as 120 days without access:

*“We reserve the right to terminate unpaid accounts that are inactive for a continuous period of 120 days. In the event of such termination, all data associated with such account will be deleted. We will provide you prior notice of such termination and backup of your data by email. The data deletion policy may be implemented with respect to any or all of the Services. Each Service will be considered an independent and separate service for the purpose of calculating the period of inactivity.”<sup>81</sup>*

Other providers have more unusual terms owing to the nature of their service. Facebook has a facility for ‘memorialising’ the accounts of users who have died, preserving the content and allowing limited posting of comments. In the case of PayPal, customer data may include electronic cash, and so a very long grace period of 3 years is applied during which PayPal will attempt to return unused funds.

Specific assurances as to data deletion are less common. One of the few examples seen is provided by 3Tera, which states in its T&C that:

*“All customer data remaining after the cancellation date will be destroyed for security and privacy reasons.”<sup>82</sup>*

Data deletion is a concern for customers who may have reservations about the degree to which a provider can assure that potentially sensitive data is no longer present in any form once it has notionally been removed from storage, or indeed once the relationship

---

<sup>80</sup> See note 43.

<sup>81</sup> See note 53.

<sup>82</sup> See note 24.

between customer and provider has come to an end. This mirrors on a larger scale existing concerns about the difficulty in ensuring that sensitive data is purged from magnetic media.<sup>83</sup>

#### 4.9. Data Disclosure

In terms of the circumstances in which providers will disclose customer information (including customer data stored on the provider's Cloud), we see a spectrum of approaches ranging from providers that have a very high threshold for justifying disclosure to ones which have a much lower one.

All providers that mention this issue<sup>84</sup> state that they will disclose such data in response to a valid court order. Some purport to establish procedural safeguards. For example, the T&C for Salesforce CRM provide that the customer will be given advance notice of a requested disclosure, unless such notice is prohibited, and that Salesforce will assist the customer in opposing such orders.<sup>85</sup>

A number of providers have a slightly lower threshold of disclosure, accepting requests (as distinct from enforceable orders) from recognised law-enforcement agencies, or where there is a clear and immediate need to disclose information in the public interest or to protect life. Facebook, for instance, will disclose customer contact information to authorities in such circumstances:

*“We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.”*<sup>86</sup>

This term is also illustrative of the relatively low threshold for disclosure espoused by some providers. G.ho.st, for instance, although now defunct, stated that it would disclose customer information if it had a ‘good faith’ belief that it would protect its own interests by doing so, whilst ADrive asserts that the decision to disclose is broadly at its discretion:

*“You authorize ADrive to disclose any information about You to law enforcement or other government officials as ADrive, in its sole discretion, believes necessary, prudent or appropriate, in connection with an investigation of fraud, intellectual*

<sup>83</sup> See, for example, ‘Have you resold your data to crooks?’, *Computerworld* 16 February 2007, [http://www.computerworld.com/s/article/9011459/Have\\_you\\_resold\\_your\\_data\\_to\\_crooks](http://www.computerworld.com/s/article/9011459/Have_you_resold_your_data_to_crooks)

<sup>84</sup> Not all those surveyed do: one provider, Zecter, is silent on the issue of third-party disclosure.

<sup>85</sup> *“The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.”* (See note 48.)

<sup>86</sup> See note 33.

*property infringement, or other activity that is illegal or may expose ADrive to legal liability.”<sup>87</sup>*

An unusual approach is that taken by IBM regarding its beta-test Smart Business Cloud. IBM expressly states that it has no duty of confidentiality regarding customer data and places responsibility for keeping it confidential on the customer, for example, via encryption:

*“...all Content and other information you provide to IBM in connection with this Agreement will be considered non-confidential. You agree that IBM has no responsibility for Content, including if Content is modified or lost. You are solely responsible for determine [sic] the appropriate procedures and controls regarding encryption and backup of all Content and for the implementation of those procedures and controls.”<sup>88</sup>*

For some Cloud services, however, disclosure may well form an inherent part of the service. As Edwards and Brown have noted, social networking sites are built upon the sharing of personal information, and are to a large extent crafted to encourage behaviour antithetical to conventional notions of privacy.<sup>89</sup> The boundary between social networking and hosting sites is increasingly blurred, with hosting sites such as Flickr offering ‘family’ and ‘friend’ contacts, special-interest groups and blogging.<sup>90</sup> Such sites will thus have to address the concerns arising from the conflicting expectations of customers who wish both to share data and to understand and control who it is shared with. The issues experienced by Facebook in particular have led to it making repeated changes to its T&C as it has sought to balance fine-grained privacy control with ease of use.<sup>91</sup> It is unlikely to be the only networking/hosting Cloud site to experience such challenges in drafting T&C appropriate to the complex and disparate needs of large user communities.

#### **4.10. Data Location / Transfer**

One of the oft-cited selling points of Cloud computing is that data and processing capacity can be flexed between a provider’s resources, potentially on a global scale. However, this has led to one of the most frequently-raised legal concerns regarding

---

<sup>87</sup> See note 25.

<sup>88</sup> For further discussion of issues surrounding the duty of confidence a Cloud computing provider may have in respect of data it hosts, see the reference at note 107.

<sup>89</sup> L Edwards and I Brown, “Data Control and Social Networking: Irreconcilable Ideas?” in A Matwyshyn (ed) *Harboring Data: Information Security, Law, and the Corporation*, Stanford Law Books, 2009; available online at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1148732](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1148732).

<sup>90</sup> <http://www.flickr.com/help/contacts/>; <http://www.flickr.com/help/groups/>; <http://www.flickr.com/help/blogging/>.

<sup>91</sup> L Hicks, “Through the Privacy Wall”, (2010) 98 *European Lawyer* 51. Before being revised in May 2010, Facebook’s Privacy Policy was, at 5,830 words, noted as being longer than the US Constitution (“Facebook mulls U-turn on Privacy”, <http://www.bbc.co.uk/news/10125260>).

Cloud computing: that a customer's data may be stored or processed in a totally different, and potentially unknown, jurisdiction.<sup>92</sup> Some major Cloud providers, such as Amazon, have made a point of offering 'regional zones' in which a customer may be assured that data will remain. Furthermore, the EU Data Protection regime acts as a strong brake on unfettered transfer of many sorts of data out of Europe;<sup>93</sup> while, conversely, US long-arm statutes may encourage attempts to avoid the jurisdictional reach of the US authorities.<sup>94</sup> As well as location, the international nature of the Cloud raises questions about the extent to which data is protected in transit, be it between the customer and provider or within the provider's own infrastructure.

Perhaps surprisingly, given the prominence often attached to these issues, few of the providers surveyed actually undertake to store data in a particular location or zone. Even Amazon does not describe its regional system in its T&C, although this feature is arguably incorporated by representation via its web-site FAQ and sign-up process.<sup>95</sup> Indeed, for the 31 sets of T&C reviewed, 15 made no mention of data location or transit protection whatsoever. Of those that did, 7 asserted compliance with US Safe Harbor procedures,<sup>96</sup> whilst some of those that did not (for example, Norton) stated that they would only transfer personal data to locations providing an equivalent or greater level of protection for personal data to that applicable where the data originated.<sup>97</sup> For one of its

---

<sup>92</sup> M Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law", (2009) 6:1 *SCRIPTed* 129, <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/mowbray.asp>; W Nauwelaerts and P Le Bousse, "Cloud Bursting", (2009) 20(4) *Computing & Law*.

<sup>93</sup> Directive 95/46/EC (OJ L 281/31, 23.11.1995), at art. 25 and 26.

<sup>94</sup> A Sachevda, "International jurisdiction in cyberspace: a comparative perspective", (2007) 13(8) *Computer and Telecommunications Law Review* 245; B Maier, "How has the law attempted to tackle the borderless nature of the internet?" (2010) 18(2) *International Journal of Law & Information Technology* 142; A C Raul, E McNicholas and E Jillson, "Reconciling European data privacy concerns with US discovery rules: conflict and comity", (2009) 2(3) *Global Competition Litigation Review* 119; C Kuner, "Data protection law and international jurisdiction on the internet", (2010) 18(2) *International Journal of Law & Information Technology* 176 (Part 1), 18(3) *International Journal of Law & Information Technology* 227 (Part 2).

<sup>95</sup> During the sign-up phase for Amazon AWS S3 a customer is offered (as of Sep 2010) one of four 'storage domains': US (Standard), US (Northern California), EU (Ireland) or Asia Pacific (Singapore). Statements, such as the comment in the Amazon S3 service description "You can choose a Region to optimize for latency, minimize costs, or address regulatory requirements ... Objects stored in a Region never leave the Region unless you transfer them out." would likely be taken under English law as representations inducing the customer to enter into a contract. Further details of Amazon's storage domain policy are available at [http://aws.amazon.com/s3/faqs/#Where\\_is\\_my\\_data\\_stored](http://aws.amazon.com/s3/faqs/#Where_is_my_data_stored).

<sup>96</sup> The 'Safe Harbour' procedure was established by the US Department of Commerce, in consultation with the European Commission, to facilitate the transfer of personal data between the EU and the US. See further <http://www.export.gov/safeharbor/>

<sup>97</sup> See, for example, section 12.2 of Norton's Privacy Policy (note 49).

online services (.Net), Microsoft mentions that it is subject to US Safe Harbor obligations but states that:

*“Personal information collected on Microsoft sites and services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of data from the European Union.”*

As well as the question of where customer data is stored, a further concern is the security of that data in transit. The international nature of Cloud services means that customer data will usually be transferred between customer and provider over the Internet. Furthermore, if (as many larger Cloud providers do) the provider has multiple data centres, then, unless the provider has built or leased its own secure network and facilities, transfers between data centres may well also be over Internet connections. Several providers (for example, 37Signals, UKFast) caution in their T&C that customer data may be transferred unencrypted over inherently insecure networks in such a manner. As 37Signals’ T&C state:

*“You understand that the technical processing and transmission of the Service, including your Content, may be transferred unencrypted and involve (a) transmissions over various networks; and (b) changes to conform and adapt to technical requirements of connecting networks or devices.”<sup>98</sup>*

By contrast, Dropbox specifically states, albeit on its website rather than in its T&C, that all data transfers are encrypted, and identifies Amazon S3 as the underlying storage service provider. It states that:

*“Dropbox takes the security of your data very seriously. Everything you store on Dropbox is encrypted both in transmission and storage. Nobody can access your files unless you choose to share them yourself.*

[...]

*Dropbox uses Amazon S3 for data storage. Amazon stores its data over several large-scale data centers. According to Amazon, they use military grade perimeter control berms, video surveillance, and professional security staff to keep their data centers physically secure.*

[...]

*All transmission of file data and metadata occurs over an encrypted channel (SSL). Any data transferred from Dropbox over the internet is securely encrypted and safe from interception and/or eavesdroppers.”<sup>99</sup>*

---

<sup>98</sup> See note 23.

<sup>99</sup> See note 31.

#### 4.11. Monitoring by Provider

It is not just disclosure of content to third parties that customers may be concerned about. Customers may equally well not wish their use of a Cloud service to be monitored by the provider, be this because such monitoring might be the precursor to third-party disclosure or because it may disclose the customer's confidential data to the provider. This latter point may still apply even if only traffic data (for example, frequency and volume of data movement) is monitored; sustained analysis of such data can reveal a considerable amount of information about the use of even encrypted services.<sup>100</sup>

Providers appear to fall into three categories in relation to their policy on monitoring the use of their services by customers. One set (including 3Tera, Google, Nirvanix and Salesforce) is silent in their T&C on the subject. This does not of course mean that they do not undertake such monitoring, only that they do not declare a policy on doing so.

A second set states that they monitor customer use, but only in terms of the nature and pattern of use (for example, bandwidth consumption) and may well state that this is specifically for the purpose of ensuring a good quality of service provision or, as Microsoft does for its SQL Azure database, for statistical analysis:

*“You also grant Microsoft the right to track and record usage patterns, trends, and other statistical data related to your use of the Services for Microsoft’s internal use.”*

The third set states that they may monitor the data the customer uploads to their Cloud, typically for purposes of enforcing their AUP (for example, Rackspace, GoGrid). It is not generally made clear in T&C whether such monitoring is proactive or in response to specific suspicions of disapproved activity; it may be that the providers do not wish to constrain themselves in this respect, or that they do not wish to assume responsibility for policing their content.<sup>101</sup> Some providers (for example, The Planet) note that they may be legally ordered to monitor customer activity without giving notice. Other providers have gone further; the now-defunct G.ho.st asserted that it reserved the right to monitor customer data without notice:

*“Ghost may, amongst its other rights, and without prior notice: [...] Monitor and analyze user's activities on the site.”*<sup>102</sup>

<sup>100</sup> S Chen *et al*, “Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow” (2010), *Proceedings of IEEE Symposium on Security and Privacy* (Oakland), IEEE Computer Society, May 2010. Available at <http://research.microsoft.com/apps/pubs/default.aspx?id=119060>.

<sup>101</sup> The degree to which Cloud providers were under a duty to actively monitor data uploaded by customers in respect of copyright infringement was the subject of a substantial claim brought by Viacom against Google regarding material uploaded to YouTube. This claim was dismissed in June 2010 but illustrates the potential for major disputes in this area. *Viacom International and ors v YouTube and ors* (23 June 2010, unreported) [http://www.google.com/press/pdf/msj\\_decision.pdf](http://www.google.com/press/pdf/msj_decision.pdf).

<sup>102</sup> See note 35.

#### 4.12. *Rights over Service / Content*

Contrary to assumptions sometimes made about Cloud providers,<sup>103</sup> this survey found no evidence of any provider seeking to assert IP rights over content and data uploaded to the Cloud by customers. Indeed, the most common term relating to IP was one stating, at greater or lesser length, that both provider and customer retained the IP to their service and data respectively. In a few cases (for example, Decho, Flexiant, Joyent) this term referred only to the provider's IP, and no mention was made to that of the customer.

A typical example of such a term can be found in the T&C for Google Apps Premier. After noting that Google retains IP in elements of its service, the T&C go on to state that:

*“Google does not own third party content used as part of the Service, including the content of third party communications appearing on the Service. Title, ownership rights and Intellectual Property Rights in and to the content accessed through the Service are the property of the applicable content owner and may be protected by applicable copyright or other law.”*<sup>104</sup>

What is seen from several providers, however, is a term asserting that the customer grants the provider a compulsory licence to republish some or all of the customer's data for the purpose of provision of the service. This is particularly so for consumer-focused services that encourage hosting as well as storage of customer content, for example, Apple and Google. Apple, for example, imposes the following licence in respect of material uploaded to iWorks:

*“License from You: Except for material we may license to you, Apple does not claim ownership of the materials and/or Content you submit or make available on the Service. However, by submitting or posting such Content on areas of the Service that are accessible by the public, you grant Apple a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available. Said license will terminate within a commercially reasonable time after you or Apple remove such Content from the public area. By submitting or posting such Content on areas of the Service that are accessible by the public, you are representing that you are the owner of such material and/or have authorization to distribute it.”*<sup>105</sup>

<sup>103</sup> See, for example, this blog post discussing the use of Cloud computing in education: ‘Heading into the cloud: cloud computing and education’, <http://blogs.educationau.edu.au/jmillea/2009/06/23/heading-into-the-cloud-cloud-computing-and-education/> in which the author states that “Some cloud services reserve intellectual property (IP) rights over everything you post so [you] may lose IP in critical materials or to collections of materials...”

<sup>104</sup> See note 37.

<sup>105</sup> See note 28.



It may be argued that this merely formalises what would be a licence implied by business efficacy or necessity, but that it does so in a way that allows the scope of the licence to be clearly established. Where variation is seen is in that scope; in particular, Facebook requires customers to grant such a licence for the use of shared content that covers a very broad range of activities, including (as has been the subject of some controversy) advertising by Facebook.<sup>106</sup>

#### **4.13. Proprietary Rights and Duties**

This topic relates specifically to terms that describe whether the contract for Cloud services gives rise to any form of non-ownership right or relationship, such as a bailment or fiduciary duties.<sup>107</sup> Here, it is easy to classify providers: the vast majority make no reference whatsoever to such a concept. Those few that do refer to proprietary rights do so in terms that on examination appear not to relate to data in the provider's Cloud. Amazon, for example, asserts that no right of bailment arises in respect of data sent to it for import into the S3 Cloud, but on close reading it is apparent that this term applies to the data when it is in the form of physical media, and that Amazon is really asserting that if a customer sends it physical data media it has no special duty of care to look after it. Similarly, The Planet appears to define customer data as 'property' but immediately goes on to assert ownership only over physical property left by the customer with it after the end of a contract. In short, the question of whether a bailment or similar such relationship exists in respect of customer data actually in the Cloud is simply not addressed by any of the providers surveyed.

#### **4.14. Warranty**

Of the elements of Cloud Provider T&C analysed by this survey, perhaps the greatest area of commonality was in respect of terms regarding the warranty given by the provider to the customer for performance of the service. Almost without exception, every provider went to considerable – and in some cases extraordinary – lengths to deny that any such warranty existed.

<sup>106</sup> 'Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."' <http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html>; N Graham and H Anderson, "Are individuals waking up to the privacy implications of social networking sites?", (2010) 32(3) *European Intellectual Property Review* 99. Although Facebook subsequently withdrew some of the most contentious terms (such as the perpetual nature of the asserted licence) it still claims a very wide range of permissible uses. From Section 2 of the Statement of Rights and Responsibilities (see Note 33): "For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your [privacy](#) and [application settings](#): you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it."

<sup>107</sup> For a discussion of the legal position regarding the ownership of data stored or processed via Cloud computing services, see Chris Reed's "Information 'Ownership' in the Cloud", [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1562461](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461).

Where there was a difference visible it was in the approach taken by those providers which asserted the law and jurisdiction of US states and those which claimed to be governed by the laws of a European country. In a clear reflection of differing commercial practices, and of differing approaches to consumer protection, US-based providers were far more comprehensive in disclaiming any warranty. For an example of a very comprehensive disclaimer, see that given by GoGrid in respect of its Cloud service:

*“GOGRID MAKES NO EXPRESS OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. GoGrid does not warrant that the Service will be uninterrupted, error-free, or free from viruses or other harmful components. The Service is provided with no warranties regarding security, reliability, protection from attacks, data integrity, or data availability (including without limitation data integrity or availability related to cloud storage features of the Service). Except to the extent specifically provided in the SLA, THE SERVICE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. No communication between Customer and GoGrid will create a warranty or in any way alter or restrict any disclaimer of warranty or limitation of liability set forth in this Section 8 or elsewhere in this Agreement.”*<sup>108</sup>

This very full disclaimer is more detailed than most others seen, but not fundamentally different from them; many providers, including Facebook and Amazon, exclude express or implied warranties that the service provided will be fit for purpose or merchantable. Some of those providers that claim European jurisdiction either do not exclude any such warranties (for example, UKFast) or accept statutory implied warranties where they apply (for example, IBM, Google). However, a number of providers claiming European jurisdiction still disclaim any such warranties (for example, Apple, G.ho.st), notwithstanding any consumer protection law to the contrary. It is worth noting that, following discussions with the UK Office of Fair Trading, Apple agreed in late 2009 to revise the T&C for its iTunes music service, in particular for terms that sought to exclude liability for faulty services or which sought to allow it unilaterally to vary the terms of the contract.<sup>109</sup> Given that many Cloud computing T&C (including Apple’s) have such terms it will be instructive to see if corresponding changes are requested in respect of them.

#### **4.15. Direct Liability**

The approaches to disclaiming warranties of service as distinct between US-based and Europe-based Cloud providers are to a large extent mirrored for terms seeking to exclude direct liability for damage caused to the customer by the provider. In this context, ‘direct liability’ is taken to mean liability for losses to the customer relating to the loss or compromise of data hosted on the Cloud service. All US-based providers surveyed seek to deny liability for direct damage as far as possible, be it in very general terms or phrased as relating to the consequences of inability to access data. Again, a

---

<sup>108</sup> See note 36.

<sup>109</sup> ‘Apple agrees to improve terms and conditions’, Office of Fair Trading 27 November 2009 <http://www.offt.gov.uk/news/press/2009/136-09>.

particularly comprehensive example can be found in GoGrid's T&C; this is long, but it is quoted here in full to illustrate the detail and extent of denial of warranty that some Cloud providers seek to impose:

*“Except to the extent specifically provided in Section 5 above, and except to the extent that applicable law specifically forbids such limitation of liability, GOGRID WILL HAVE NO LIABILITY WHATSOEVER FOR ANY CLAIMS, LOSSES, ACTIONS, DAMAGES, SUITS, OR PROCEEDINGS RESULTING FROM ANY OF THE FOLLOWING OR FROM ANY GOGRID EFFORTS TO ADDRESS OR MITIGATE ANY OF THE FOLLOWING: (i) SECURITY BREACHES, INCLUDING WITHOUT LIMITATION EAVESDROPPING, THIRD PARTY ACCESS TO CUSTOMER DATA OR TO ASSIGNED COMPUTERS, THIRD PARTY ACCESS TO OR MISUSE OF PASSWORDS PROVIDED TO GOGRID, AND INTERCEPTION OF TRAFFIC SENT OR RECEIVED USING THE SERVICE; (ii) RELEASE OR EXPOSURE, FOR ANY OTHER REASON, OF PERSONALLY IDENTIFIABLE INFORMATION OR OTHER PRIVATE DATA, INCLUDING DATA BELONGING TO CUSTOMER'S OWN CUSTOMERS AND OTHER USERS; (iii) DENIAL OF SERVICE ATTACKS, VIRUSES, WORMS, AND OTHER INTENTIONAL INTERFERENCE BY THIRD PARTIES, INCLUDING WITHOUT LIMITATION BY OTHER GOGRID CUSTOMERS; (iv) LOSS OF DATA OR LOSS OF ACCESS TO DATA; (v) ACTIONS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION OTHER GOGRID CUSTOMERS AND THIRD PARTY PRODUCTS AND SERVICES PROVIDERS; (vi) ACTIONS OF GOGRID EMPLOYEES, AGENTS, OR CONTRACTORS ACTING OUTSIDE THE SCOPE OF THEIR DUTIES; (vii) MISTAKES, OMISSIONS, INTERRUPTIONS, DELETIONS OF FILES, ERRORS, DEFECTS, DELAYS IN OPERATION, OR OTHER FAILURES OF PERFORMANCE OF THE SERVICE, INCLUDING WITHOUT LIMITATION ACCIDENTAL DISCONNECTION AND TERMINATION OF SERVICE; AND (viii) THE ACCURACY, COMPLETENESS, AND USEFULNESS OF THE SERVICE. THE PROVISIONS OF THIS SUBSECTION 8(c) APPLY, WITHOUT LIMITATION, EVEN IF CUSTOMER PURCHASES SERVICE FEATURES ADDRESSING SECURITY, DATA INTEGRITY, DATA BACKUP, ATTACK PROTECTION, VIRUSES, SPAM, MONITORING, OR SYSTEM INTEGRITY”<sup>110</sup>*

What is notable about this disclaimer of warranty is that it purports to apply even where the customer has specifically contracted for services of the kind for which warranty is excluded.

Providers based in Europe tend to be less overt about seeking to exclude direct liability, presumably on the basis that in most European legal systems it is difficult to do so. Such exclusions as there are tend to be based on, for instance, *force majeure* (as with Flexiant or ElasticHosts). Flexiant states, for instance:

---

<sup>110</sup> See note 36.

*“We are not liable for any loss or damage that you may suffer because of any: act of God; power cut; power surge; trade or labour dispute or shortage, terrorist attack, illness or pandemic, act, failure or omission of any government or authority; power surge or power loss [sic];<sup>111</sup> obstruction or failure of telecommunication services; or any other delay or failure caused by a third party. In such an event, we reserve the right to cancel or suspend the Website and/or our Services without incurring any liability.”<sup>112</sup>*

#### **4.16. Indirect Liability**

Disclaimers against indirect liability, such as for indirect, consequential or economic losses arising from a breach by the provider, are even more common. This is no doubt due to the potentially very large scope of such damages. It may prove difficult to quantify the direct loss, if any, resulting from the deletion of customer data by a Cloud provider. However, if that data is essential to, for instance, the operation of a busy online retail system, the resulting loss of business may be very large. As such, with the exception of Flexiant, which did not make a specific reference to such losses, every single provider surveyed specifically excluded them. Such variations as there were related to detail, for example, excluding indirect losses that were specifically within the contemplation of both parties.<sup>113</sup> To quote UKFast’s T&C for CloudHosts:

*“...in no case will the Company be liable to the Customer [or] any third party for or in respect of any indirect or consequential loss or damage (whether financial or otherwise) or for any loss of data, profit, revenue, contracts or business however caused (whether arising out of any negligence or breach of the Agreement or otherwise) even if the event was foreseeable by, or the possibility thereof is or has been brought to the attention of the Company.”*

Whether such terms will be effective is another matter, however. The question of remoteness and foreseeability of loss for the purposes of exclusions in IT contracts was addressed by the English High Court in *GB Gas Holdings v Accenture* [2009] EWHC 2966 (Comm).<sup>114</sup> The Court held that a number of the claimant’s business losses arising from the defendant’s delay in implementing the contract were in fact direct losses occasioned by the breach of contract. Cloud computing contracts that seek to define

<sup>111</sup> Redundant and repeated language present in original.

<sup>112</sup> See note 34. This term was updated by Flexiant in the course of the writing of this paper. The original term, prior to a revision dated 10 April 2010, was as follows; it was less specific, but conveyed the same intent:

*“We shall not be in breach of the Agreement or otherwise liable to you in any manner whatsoever for any failure or delay in performing our obligations under the Agreement due to force majeure. [...] In these terms and conditions “force majeure” shall include, but is not limited to, such causes beyond our control, and without our fault or negligence...”*

<sup>113</sup> In English law, *Hadley v Baxendale* ‘Limb 2’ losses.

<sup>114</sup> The decision was upheld in the Court of Appeal, [2010] EWCA Civ 912.

losses consequential on service failure as being indirect and then attempt to exclude them may therefore not, at least if litigated upon in an English court, insulate the provider from wider liability for such losses.

#### **4.17. Limit of Liability**

Notwithstanding the denial of warranties and exclusions of liability commonly seen throughout the surveyed T&C, it is also common to find terms seeking to limit the extent of any damages that the provider is held liable for.

The majority of providers surveyed (19 of the 31 T&C analysed) take the approach of setting a maximum liability that is some multiple of the amount paid in service fees by the customer over a set period, often with an upper limit. For example, GoGrid and Salesforce CRM limit their liability to the total amount paid by the customer over the previous 12 months; Rackspace to 12 times the monthly fee, and UKFast and ElasticHosts to only one month's fees. Decho, which offers both paid and free services, limits its liability to the total amount paid by the customer, and specifically notes that for free services this equates to a total denial of liability:

*“WITHOUT LIMITING THE FOREGOING, THE TOTAL AGGREGATE LIABILITY OF DECHO, AND ITS SUPPLIERS, RESELLERS, PARTNERS AND THEIR RESPECTIVE AFFILIATES ARISING FROM OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT, IF ANY, PAID BY YOU TO DECHO FOR THE SOFTWARE OR SERVICES. IF THE SOFTWARE AND SERVICES ARE PROVIDED WITHOUT CHARGE, THEN DECHO AND ITS SUPPLIERS SHALL HAVE NO LIABILITY TO YOU WHATSOEVER.”<sup>115</sup>*

Seven of the providers surveyed do not specify a liability limit but deny all direct and indirect liability (see the discussion above); it has thus been assumed that in effect they simply deny liability to any extent whatsoever.

Where a flat liability is specified, be it as a general limit or as a cap to a pro-rata liability, the amount varies significantly depending on the nature of the provider's service and the expected customers for it. ADrive, which offers consumer storage service, has a liability limit of US\$100, as do Dropbox and Facebook; UKFast, a host catering to SMEs, a liability limit of £5,000, and IBM a liability limit for European customers of Euro 500,000.<sup>116</sup> IBM's T&C are, in this respect, an interesting example of localisation, with the section on limitation of liability having extensive regional variations as to the detailed provisions of how such limits apply.

#### **4.18. Indemnification**

As well as seeking to deny or strictly limit liability, most Cloud providers incorporate indemnification clauses into their T&C. For 24 of the 31 T&C analysed, the customer is required to indemnify the provider against any claim against the provider arising from the

---

<sup>115</sup> See note 30.

<sup>116</sup> See notes 25, 31, 33, 51 and 39 respectively.

customer's use of the service. From the consumer or SME perspective, it is worth noting that such terms are imposed not only by providers that charge for Cloud services but also by the free-to-use service providers surveyed such as Dropbox and Facebook. As of the time of drafting this paper, for instance, some 500 million Facebook users, none of whom pay for the service they use, have by signing up agreed to the following indemnification term:

*"If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim."*

Conversely, a number of providers undertake to indemnify the customer in certain circumstances. Four providers – 3Tera, Akamai, Google (for Google Apps Premier) and Salesforce (for Salesforce CRM) – indemnify the customer against claims brought against them for IP infringement arising from use of the provider's service. 3Tera's indemnification clause, for instance, states:

*"Each party agrees to indemnify and hold harmless the other party, the other party's affiliates, and each of their respective officers, directors, attorneys, agents, and employees from and against any and all claims, demands, liabilities, obligations, losses, damages, penalties, fines, punitive damages, amounts in interest, expenses and disbursements of any kind and nature whatsoever (including reasonable attorneys' fees) brought by a third party under any theory of legal liability arising out of or related to the indemnifying party's actual or alleged infringement or misappropriation of a third party's copyright, trade secret, patent, trademark, or other proprietary right."*

Such a claim would typically be one brought for IP infringement in relation to the provider's technology.<sup>117</sup> This indemnity may be stated to be conditional; for instance, Google Apps Premier's indemnification clause requires the customer to allow the provider to control the course of litigation.

#### **4.19. Service Credits**

Although many providers seek to deny or limit liability, a number (particularly those offering commercial services) provide a mechanism for compensating customers for failure to deliver the service to set levels. Such compensation is invariably by service credit, allowing the customer a rebate against future billing; no exceptions were found to this in all the providers surveyed. Both ElasticHosts and GoGrid, for example, offer service credits of 100 times the cost of the lost service (for example, a six-minute outage would attract a rebate of 10 hours' service charges) capped at one month's service

<sup>117</sup> For example, the recently-emerging (as of the drafting of this paper) legal dispute between Microsoft and Salesforce.com over patents for Cloud Computing Technology; 'Salesforce countersues Microsoft in patent spat', ZDNet, 28 June 2010, available at <http://www.zdnet.co.uk/news/intellectual-property/2010/06/28/salesforce-countersues-microsoft-in-patent-spat-40089365/>.

fees.<sup>118</sup> The Planet offers a more complex rebate mechanism, with customers receiving a 5% monthly fee rebate for the first 5 minutes of lost service, and then a further 5% for each additional 30 minutes; this presumably recognises that service failures that last more than a few minutes may be quite prolonged.<sup>119</sup>

Service credits are typically governed by a separate Service Level Agreement, which will usually exclude such causes of downtime as scheduled maintenance or any factors outside the provider's immediate control, such as routing or traffic issues affecting Internet links (see the discussion below of terms relating to 'service availability').

Service credits may also be offered under very restrictive conditions; for example, ElasticHosts specifies that it will be sole arbiter of the eligibility for and extent of credits, and that they are the sole remedy available to the customer for service deficiency.<sup>120</sup>

#### **4.20. Service Availability**

Where a provider offers service credits, it will specify a service performance target that it will aim to meet. This target may often appear quite optimistic – Flexiant, Joyent and The Planet all set 100% service uptime targets – but as noted in the discussion of service credits, this target will usually exclude a wide range of potential causes of loss of service. ElasticHosts, for example, states a 100% availability target but excludes the following sources of potential downtime:

*“Your payments not covering your use, including but not limited to when your subscriptions or prepaid balance run out.*

*Acts or omissions of you or your users.*

*Software running within your virtual servers.*

*Scheduled maintenance which we have announced at least 24 hours in advance.*

*Factors outside our control, including but not limited to any force majeure events; failures, acts or omissions of our upstream providers or failures of the internet.*

*Actions of third parties, including but not limited to security compromises, denial of service attacks and viruses.*

*Violations of our Acceptable Use Policy.*

*Law enforcement activity.”*<sup>121</sup>

---

<sup>118</sup> See notes 32 and 36.

<sup>119</sup> See note 50.

<sup>120</sup> *“We will be the sole arbiter regarding the award of credit and our decision will be final and binding. The award of credit by us to you as described in this Service Level Agreement will be the sole and exclusive remedy for unavailability of stored data or virtual servers or loss of stored data. Credits will only be provided against future service and for the avoidance of doubt may not be exchanged for cash or other forms of payment”* (See note 32.)

Conversely, many providers expressly disclaim any availability target. Fifteen of the 31 T&C analysed incorporated terms by which the provider stated that the service was 'as-is' or 'best-efforts', or that it may be suspended or discontinued at any time. Decho, for instance, states that:

*“Decho reserves the right at any time to modify, suspend, or discontinue providing the Service or any part thereof in its sole discretion with or without notice.”*<sup>122</sup>

Although Mozy offers both consumer (free and paid) and business (paid) services, their T&C are virtually identical and this clause appears in both. Indeed, such terms were seen across the full range of Cloud services covered by this survey, ranging from those aimed at consumers to those, such as Amazon Web Services, aimed at a market primarily of other Cloud providers.

## 5. Analysis

### 5.1. Evolution of Terms of Service

From the outset it was intended that provider T&C would be archived and regularly revisited so as to allow their development to be monitored. The intent of this is to allow for the analysis not only of T&C themselves but also their evolution, with the aim of identifying any broad trends.

This paper has been based upon T&C as sampled in early January 2010. In mid-June 2010, as this paper was in its final draft stage, the T&C for all the providers covered by the survey were revisited, save for G.ho.st, which had ceased operation during this period. For each provider, all T&C documents were examined to see whether they had been changed since the initial sample and the extent, if at all, to which changes had been highlighted to users.

It will be apparent that there are four possible statuses for each document:

- *Changed and Notified*: This means that the document had changed since the January 2010 sample and that there is notice of this within the document, e.g. an issue date more recent than this. 18 documents were in this category, representing 11 providers. 15 of those documents were from 8 providers that either put the customer on notice to review terms or made no mention of policy for contract variation. As such a diligent customer would note that there had been a change, although in no case was there a positive indication (e.g. by highlighting) of what the change had been.
- *Unchanged and Notified*: This means that the document contained an issue date that was before January 2010 and which indeed matched that of the previous sample copy of that document. 28 documents were in this category, representing

---

<sup>121</sup> *ibid.*

<sup>122</sup> See note 30.



18 providers. 16 of those documents were from 10 providers that either put the customer on notice to review terms or made no mention of policy for contract variation. A customer seeking to confirm the status of his or her T&C could thus readily discern that these documents had not changed.

- *Unchanged and Not Notified:* This meant that there was no indication of the change status or last issue date of the document in question, but that comparison of the most recent copy with the one archived in January 2010 revealed no changes. 19 documents from 12 providers were in this category. 14 of those documents were from 8 providers that either put the customer on notice to review terms or made no mention of policy for contract variation. Customers of these providers are thus faced with a careful review of often lengthy T&C documents to reassure themselves that there has been no contract variation.<sup>123</sup>
- *Changed and Not Notified:* These documents also had no indication of change status or last issue date, but comparison with the January 2010 version revealed subsequent changes. 4 documents from 3 providers were in this category. 3 of those documents were from 2 providers that either put the customer on notice to review terms or made no mention of policy for contract variation. As such there were changes that a customer could only have discovered by regular diligent review of the published T&C. (The one document that was from a provider that said it would notify customers of changes had a minor change in terminology that the provider presumably did not consider worthy of notification.)

It is worth noting that many of the providers that lacked a positive notification policy did nonetheless make it clear when their published T&C had last changed, usually by including a review date. (In some cases, as noted, the changes were very minor; nonetheless, it is useful for customers to see that the document has been at the very least reviewed recently.) However it is a matter of concern that such a policy is not universal. In particular, where a provider places the burden of monitoring its T&C for changes onto its customers, it would seem incumbent upon it to make it clear if such changes have actually taken place. Even those that did date their T&C did not, for instance, mark up revised passages or note specific changes. Were a provider to update its AUP without making it clear to its customers that it had done so, some customers could find that hitherto permitted activities were now proscribed.<sup>124</sup>

## 5.2. Comparing and Categorising T&C

One of the overarching aims of this analysis was to identify and evaluate patterns in the T&C offered by the providers covered by this survey. Both common features and

---

<sup>123</sup> In the case of some T&C documents we resorted to document version comparison software to identify if changes had been made.

<sup>124</sup> Although if the AUP was amended to reflect legislative changes (e.g. to restrict behaviour newly made illegal) the provider could argue that the customers had not been disadvantaged in that such behaviour was now proscribed by law. Nonetheless it would seem prudent to ensure that customers were advised of such changes.

distinctive approaches were noted. The patterns that emerged fall into three main categories:

- Aspects of the T&C that are distinctly segmented among providers; in other words, some providers adopt one approach to such terms, whilst others take a clearly different one.
- Aspects of the T&C where the opposite is seen, with most or all providers adopting a common approach to a particular area of T&C.
- Areas of T&C where most or all providers take a common basic approach but some then develop this approach further. This is termed a 'spectrum' approach, in that providers are seen to lie on a spectrum of greater or lesser variation from a default position.

In respect of the first type of T&C term, the clearest segmentation among Cloud providers is that between those for services that are explicitly paid for and those which are free, or at least not funded by direct subscription. Such a distinction is not surprising as the obligations of a provider are likely to be in proportion to the consideration provided by a customer. This is most clearly seen in respect of data retention beyond the termination of the customer/provider relationship. Such retention requires the provider to commit resources such as storage and account management; indeed, even if access is provided only for the customer to withdraw data, this requires effort on the part of the provider as non-standard access to the Cloud is required.

Another clear distinction observed was between providers that asserted that their T&C were governed by the law of US states and those that claimed to be covered by the laws of European countries. Very extensive disclaimers of warranty or limitations of liability were much more common among the former than the latter. Again, this is not a surprising distinction. European legal systems tend to be less tolerant than those of US states regarding terms that limit the duty of one party, particularly if it is the more powerful one, to perform its obligations under a contract. This is most clearly enshrined in EU law in respect of consumer transactions, such as the Unfair Contract Terms Directive<sup>125</sup> and Distance Selling Directive.<sup>126</sup>

A more general distinction observed is that between SaaS products and IaaS products. Put simply, the T&C of various IaaS products tend to resemble one another more than those of SaaS products. This again is readily explicable; IaaS providers are selling the computing equivalent of raw commodities – processing power, storage capacity and bandwidth. Although the exact details of a virtual machine may vary between two providers, both are selling what in essence is the same product. By contrast, a SaaS

---

<sup>125</sup> Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

<sup>126</sup> Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ L 144, 4.6.1999, p. 19).

provider offering an online document processing service is selling something very different from one offering Cloud-based customer management services.

Other areas where providers fell into clear groups in respect of their T&C include monitoring of customer activity and variation of the T&C themselves. In respect of monitoring, providers adopt one of three approaches: they do not state that they do so,<sup>127</sup> note that they do so for the claimed purpose of maintaining service quality,<sup>128</sup> or claim to do so explicitly so as to police their AUP.<sup>129,130</sup> Although there is no clear segmentation in the market in terms of approach to monitoring, there is an apparent predominance of IaaS hosting providers in the third group

As for T&C variation, there is a division between those providers that state that they will provide written notice (in some cases even conditional on mutual acceptance) and those which require the customer to monitor published T&C for unilateral changes. Here, it was noticeable that the former group included providers such as Salesforce and Iron Mountain that provide SaaS products in areas such as CRM and archiving where long-term trusted customer relationships are important.

In respect of the second type of T&C term, that which varies little between providers, the clearest example is seen by comparing the AUP for Cloud services. At first sight there seems to be significant variations between them; the AUP for 37Signals, for instance, simply reserves the right to delete content that is “unlawful, offensive, threatening, libellous, defamatory, pornographic, obscene or otherwise objectionable”<sup>131</sup> whereas that for Rackspace is a lengthy separate document.<sup>132</sup> On closer inspection though, Rackspace’s AUP prohibits fundamentally the same set of behaviours as 37Signals’; it is just that one AUP goes into much more detail in describing them than the other. This pattern is seen across the providers covered by this survey; without exception every provider incorporates some form of AUP in its T&C, and for the most part these consistently prohibit broadly the same set of activities that fall outside the generally accepted bounds of legitimate conduct in the European/US marketplace that was covered in this survey.<sup>133</sup>

---

<sup>127</sup> 37Signals, 3Tera, Akamai, Google, IBM, Nirvanix, PayPal, Salesforce, Zectar and Zoho make no mention of monitoring. UKFast states that it will not proactively monitor customer compliance with the AUP.

<sup>128</sup> Apple, Decho, Dropbox, Facebook, Flexiant and Microsoft.

<sup>129</sup> Adrive, Amazon, Elastichosts, Ghost (now defunct), GoGrid, Joyent, Rackspace, Symantec and The Planet.

<sup>130</sup> It is of course possible that providers that make no mention of a monitoring policy in their T&C nonetheless do so for either of the reasons quoted.

<sup>131</sup> See note 23.

<sup>132</sup> See note 47.

<sup>133</sup> The AUP for Decho Mozy is extremely brief and general; it simply requires the customer to use the service “...in compliance with all applicable laws, rules and regulations.” (See note 30.)

A further area of consistency is in the approach providers take to limiting their liability to customers. Where such liability is not denied altogether, it is typically subject either to a flat amount or a ceiling described in terms of the total amount paid by the customer over a period ranging from the previous month to the previous year. It is also common to see terms that seek to exclude any express or implied warranty for fitness for purpose, or for indirect losses arising from use of the provider's service. Where the provider issues an SLA, this also usually excludes responsibility for service outages from such causes as scheduled maintenance or Internet connectivity problems. Such SLAs also invariably limit the remedy available to customers to a credit specifically against future use of the provider's service.

As for the third type of T&C term, the 'spectrum' of approaches, a good example is seen in the policy that providers say they will take towards requests for disclosure of customer data. Of the providers that address this point, all say that they will give such disclosure in response to an enforceable order of a court of competent jurisdiction. However, some go further and say that they will disclose customer data on mere request from government and law-enforcement agencies, with a few going even further than that and stating that they will disclose customer data where they consider it is in their business interests to do so.

Another example of a 'spectrum' term is in relation to IP rights over customer data. Those providers that state a policy in this area state that the customer retains ownership of the IP in its data and content. However, some providers then go on to impose via the T&C a licence by which the customer authorises the provider to copy such data and republish it for the purpose of providing the service. Again, at least one provider (Facebook) goes further in specifying a range of uses it may then put such data to.

### **5.3. T&C – What a Prospective Customer Should Expect**

A prospective customer of Cloud computing services may ask if this analysis sheds any light on the nature of the T&C that should or could be expected. As the discussion above notes, it is indeed possible to discern patterns in Cloud T&C and at a minimum these may act as a guide to what a reasonable range of terms may be in a particular area of a contract. For example, a customer seeking to enter into a paid contract for IaaS provision should, on the basis of the T&C examined, reasonably expect a clause limiting liability to between one month's and one year's total customer payment; a total denial of liability would be less usual. Similarly, such a prospective customer should be aware that the SLA will almost certainly limit remedies for service outages to a rebate against future billing for the service in question.

The following points are noted as general guidance, as a checklist of points to bear in mind when examining Cloud T&C:<sup>134</sup>

- Cloud service providers will generally, but not invariably, use their principal place of business as the basis for the legal system and litigation forum governing their

<sup>134</sup> They are emphatically not legal advice and do not and should not provide a substitute for careful examination of the T&C of a Cloud service, and professional legal advice if appropriate.

T&C. This means that many Cloud services are offered under the law of US states and subject to terms that purport to restrict legal disputes to the courts of those states. Some larger providers, however, have localised legal frameworks. Customers may be more comfortable with the prospect of signing contracts governed by legal systems for which they can more readily obtain advice and which expressly provide for more local resolution of disputes.

- Most Cloud providers will seek to exclude, as far as possible under the legal system applying to the contract, any warranty of service or acceptance of liability. Such liability as cannot be disclaimed altogether will typically be strictly limited. Those providers asserting that their T&C are governed by the laws of US states will generally have more wide-ranging disclaimers of liability than those which claim to be governed by, for instance, English law or the law of other EU states.
- Customers should consider carefully terms by which the provider seeks to allow itself to vary the T&C unilaterally, or to impose termination conditions for the contract based on criteria for which it is the sole arbiter.
- Where a prospective customer has specific security concerns, the T&C should be consulted to assess the provider's approach to securing and protecting data. Those customers wishing to use a Cloud-based solution for backup of important data should in particular take note of terms by which a provider advises or requires customers separately to back up data placed on their Cloud service (in other words, where the proposed backup solution itself disclaims responsibility for being a reliable backup).
- Data protection and privacy issues need to be considered via careful scrutiny of T&C, not least because exclusions and disclaimers relating to them may well, on the evidence of this survey, not be exclusively in the part of the T&C specifically labelled as relating to privacy. The threshold for disclosure and policy regarding monitoring of customer activities can both vary considerably from provider to provider. Furthermore, few providers are explicit as to the location or even general zone that data is stored in, or the identity of any underlying service providers; if such considerations are important to a customer (for example, where there is a risk that personal data may be exported from the EEA) then if the T&C are not clear on the point further investigation would be advisable.
- Data retention post termination of the contract is an area where providers differ sharply in approach. 'Free' services may often not provide such retention; if coupled with termination clauses that allow the provider to terminate the relationship at its own discretion with little or no notice, this may result in the risk of the customer losing access to all data. Paid services generally allow a grace period but customers should check to ensure how long this lasts and whether there might be, for instance, additional costs involved.
- Care should be taken in selecting a Cloud service on the basis of features or policies that are not specifically mentioned in the T&C. Unless such a feature is

clearly referred to in the process of signing up to the service it may not comprise either a term of the agreement or a representation deemed to have induced it.

## 6. Conclusions

Much of the attention so far given to Cloud computing has focussed on the underlying technologies and on services that can be enabled or facilitated by Cloud computing. Increasingly, however, the legal issues that may arise from use of Cloud computing are gaining prominence. The papers being produced in the course of the QMUL Cloud Legal Project, including this paper, are intended to address many such issues.

Our examination of the T&C for a broad range of Cloud services has revealed both common elements and contrasts. Many Cloud providers include elements in their T&C asserting wide-ranging disclaimers of liability or of any warranty that the service will operate as described, or indeed at all. SLAs will often be couched in such terms as to exclude the majority of causes of a Cloud service outage, and will provide remedies only in the form of credits against future service. Conversely, prospective customers may find that the threshold for disclosure to a third party, the extent to which data will be preserved following the end of a contract and the legal system under which the contract is offered will vary greatly from provider to provider.

On the basis of our initial analysis some patterns can be discerned. Where a customer explicitly pays for a service, the provider is likely to provide more in the way of remedies for service outages (albeit usually subject to heavy caveats) and will often facilitate access to data post-termination of a contract. Those providers based in Europe or which assert the law of a European state for customers in Europe will typically be less forceful in denying liability than those which are based in, and assert the legal governance of, a US state. And while the terms governing acceptable (or rather unacceptable) use of a service may seem to vary widely, in practical terms they usually proscribe a very similar list of activities.

How are Cloud T&C likely to develop? We have already noted<sup>135</sup> that the complex and often conflicting expectations of users of social networking sites can force the rapid evolution of T&C, especially in customer-sensitive areas such as privacy. Where providers of hosting and utility services aimed at consumers seek to incorporate elements of social networking into their products they are likely to encounter similar pressures. We anticipate that producing T&C that are clear, comprehensive and concise in respect of matters such as privacy will provide an ongoing challenge and further work should be undertaken to monitor and assess the evolution of such terms.

Another area likely to be of growing interest to consumers, but also of importance to enterprise and government customers, is the approach providers take to resolution of disputes. Our research has found extensive use of terms seeking to impose arbitration or the provider's choice of law and forum for litigation. Although such terms may be ineffective against consumers they may still pose obstacles to customers with a grievance. It avails a customer little to be told that she can, notwithstanding a Cloud

---

<sup>135</sup> See section 4.9.

provider's T&C, sue that provider in her local court if the chances of obtaining an enforceable judgment against it are minimal because all its business and assets are in a remote jurisdiction. Such issues are of course not new but, as with so many of the legal concerns arising from Cloud computing, the nature of Cloud business makes it easier for ordinary users to encounter them. As the use of global Cloud services grows it is likely that more customers will find themselves party to international disputes regarding services delivered to their desktop or mobile; whilst the Cloud may be location-independent, legal remedies are not.<sup>136</sup> Enterprise and government customers may be in an even more difficult position, as they will not be shielded by consumer protection laws.

One scenario is that consumer customers accustomed to strong legal protection in disputes may start to see Cloud services as carrying a risk of lacking an accessible and enforceable dispute resolution mechanism, whilst corporate customers become wary of T&C that impose unfamiliar legal systems. The widespread exclusion of liability claimed in many T&C is likely to aggravate such concerns.

Providers may seek to reassure customers by tailoring T&C to conform more closely with local expectations. We have already seen such 'localisation' in the T&C of some of the providers surveyed in this paper.<sup>137</sup> Large providers may make a virtue of offering locally-tailored T&C, whilst smaller, local providers may seek to emphasise their connection to the jurisdiction of their customers.<sup>138</sup>

If a significant number of providers do adapt or localise their T&C to counter potential or actual customer concerns we may see a 'virtuous circle' setting in through customer pressure. Once customers start to note that some providers offer T&C that offer more in the way of enforceable rights than others do, the presence or absence of such rights may well become a selling point. Alternatively, public or administrative law intervention or regulatory pressure may be brought to bear against providers to ensure that, for example, European consumers are offered T&C that are compliant with EU consumer protection law.

The Cloud T&C element of the QMUL Cloud Legal Project is an ongoing endeavour and we will continue to monitor changes to the private law terms on which such services are offered. As the Cloud marketplace expands and matures we expect such terms to evolve and diversify to more closely reflect both customer concerns and the local legal framework under which those customers operate.

---

<sup>136</sup> Although a provider might assert that it was acting in the best interests of customers by imposing arbitration on the basis that a recognised arbitration procedure and forum is more likely to be accessible to a customer than the legal system and courts of a foreign Cloud provider. Nonetheless, consumer protection law may view such imposed arbitration as unfair, as per note 66

<sup>137</sup> See Section 4.17.

<sup>138</sup> Indeed, as noted at Section 4.2, Flexiant specifically asserts Scottish law as governing its T&C.