STANFORD TECHNOLOGY LAW REVIEW
VOLUME 16, NUMBER 1 FALL 2012

NEGOTIATING CLOUD CONTRACTS: LOOKING AT CLOUDS FROM BOTH SIDES NOW

W. Kuan Hon, Christopher Millard & Ian Walden*

CITE AS: 16 STAN. TECH. L. REV. 79 (2012)
http://stlr.stanford.edu/pdf/cloudcontracts.pdf

ABSTRACT

Contract terms for cloud computing services are evolving, driven by users' attempts to negotiate providers' standard terms to make them more suitable for their requirements, as well as market developments, particularly among cloud integrators. This Article, drawing on sources including interviews with cloud computing providers, users and other market actors, is the first in-depth research into how cloud contracts are negotiated. In particular, we have focused on instances where users have requested changes to providers' standard terms, and the extent to which providers agreed to those changes. We have found that the terms that generated the most negotiation were provider liability, service level agreements, data protection and security, termination rights, unilateral amendments to service features, and intellectual property rights. Changes to providers' standard terms are likely to filter down from large deals where users have negotiated amendments, and filter up from regulatory action affecting the consumer market. This Article suggests a multiplicity of approaches are emerging, rather than a de facto 'cloud' model, with market participants developing a range of cloud services with different contractual terms, priced at different levels, and embracing standards and certifications that aid legal certainty and compliance, particularly for small

* The authors are, respectively, a consultant to the QMUL Cloud Legal Project, Professor of Privacy and Information Law at the Centre for Commercial Legal Studies, Queen Mary, University of London, and Professor of Information and Communications Law at the Centre for Commercial Legal Studies, Queen Mary, University of London. This Article was written as part of the QMUL Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary, University of London. The authors are very grateful to their sources—most of which wished not to be named—for their participation and assistance in this research. The authors are grateful to Microsoft for generous financial support making this project possible. Views herein, however, are solely the authors'.

and medium-sized enterprise users.

INTRODUCTION

The top ten strategic technology trends for 2013 include, are based on, or

incorporate cloud computing; those trends include personal cloud, hybrid information technology and cloud computing, cloud-based analytics, in memory computing and integrated technology ecosystems.[1] However, the cloud market is still relatively immature. The state of providers' standard contract terms seems to reflect this. In a 2010 survey of some thirty standard terms of cloud providers,[2] most terms surveyed were found, unsurprisingly, to be weighted in favor of the provider, and many were potentially non-compliant, invalid, or unenforceable in some countries.

This Article summarizes our subsequent qualitative research into negotiated cloud contracts, where users have requested changes to providers' standard cloud contract terms and the extent to which providers agreed those changes. Based on our research, users consider that providers' standard contract terms or offerings do not sufficiently accommodate customer needs in various respects. The top six types of terms most negotiated, according to our sources, were as follows, with the third and fourth issues ranking roughly equally in importance (depending on type of user and service):

1. exclusion or limitation of liability and remedies, particularly regarding data integrity and disaster recovery;
2. service levels, including availability;
3. security and privacy,[3] particularly regulatory issues under the European Union Data Protection Directive;[4]
4. lock-in and exit, including term, termination rights, and return of data on exit;
5. providers' ability to change service features unilaterally; and
6. intellectual property rights.

This Article proceeds as follows: in Part I we describe our research methodology and the scope of our analysis. Then, in Part II, we outline providers' perspective on cloud contract terms. Next, in Part III, we discuss users' perspective on cloud contracts, including factors that influence why users request

---

1. *Gartner Identifies the Top 10 Strategic Technology Trends for 2013*, GARTNER NEWSROOM (Oct. 23, 2012), http://www.gartner.com/it/page.jsp?id=2209615

2. Simon Bradshaw, Christopher Millard & Ian Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, 19(3) INT'L J.L. & INFO. TECH. 187 (2011).

3. *See* Cloud Industry Forum, *Cloud UK: Paper One Adoption and Trends 2011* (2011) [hereinafter *CIF1*], *available at* http://www.cloudindustryforum.org/downloads/whitepapers/cif-white-paper-1-2011-cloud-uk-adoption-and-trends.pdf (62% of enterprise decision-makers polled cited data security, and 55% data privacy, as their biggest concerns with cloud adoption); *cf.* Cloud Industry Forum, *Cloud UK: Paper Four Cloud Adoption and Trends for 2012* (2011) [hereinafter *CIF4*], *available at* http://www.cloudindustryforum.org/downloads/whitepapers/cif-white-paper-4-cloud-adoption-and-outlook-for-2012.pdf (these figures were 64% and 62% respectively, in a Cloud Industry Forum poll conducted one year prior).

4. Council Directive 95/46/EC, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

certain terms and why providers may agree to them, including the role of systems integrators. In the course of that analysis we discuss in detail the key types of terms negotiated. Finally, we conclude with how cloud contracts are likely to develop as the cloud market matures.

I. METHODOLOGY AND SCOPE

This Article offers a qualitative analysis of negotiations of cloud computing contract terms[5] over a particular time period. Our sources discussed specific deals they had been involved with, and their experiences and personal views. Some providers and law firms provided generalized experiences regarding users and clients. From our research, this Article identifies themes regarding cloud contracts that we believe are reasonably representative of the key issues of concern in the cloud market at this relatively immature stage of cloud adoption.

Our sources comprised reports of experiences at various public conferences and seminars, or in informal discussions with cloud actors, plus detailed confidential interviews[6] with over twenty organizations[7] of at least an hour each, conducted between December 2010 and early 2012. Our interviewees included: cloud providers, such as United Kingdom-based or global software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) providers, including integrators, and European Union and non-European Union telecommunications providers; cloud users, such as businesses serving consumers, financial services businesses, and United Kingdom public sector and educational organizations; and other cloud market actors, such as law firms and insurance industry firms.[8]

This Article analyzes only contracts between cloud users and providers of

---

5. In discussing negotiated contracts with our sources, we relied solely on the information these sources provided regarding their contracts. Generally, we were not able to verify terms as stated, since contracts were confidential to the parties. Not all types of terms were discussed with every source, as some users had not yet reached the stage of needing to scrutinize certain terms (e.g., ongoing audit rights).

6. Most interviewees were United Kingdom-based, and from legal rather than information technology departments. In some organizations, we spoke to both legal and technical experts.

7. For qualitative research purposes, fifteen to twenty interviews generally is considered adequate to obtain a good range of views before reaching "saturation," the point where no new information or themes are observed in the data and the same information starts recurring. *See, e.g.*, Greg Guest, Arwen Bunce & Laura Johnson, *How Many Interviews Are Enough? An Experiment with Data Saturation and Variability*, 18 FIELD METHODS 59 (2006). We did not attempt any quantitative surveys, although we reference certain surveys carried out by others, such as the Cloud Industry Forum.

8. We do not provide more detailed breakdowns, as that could identify those who agreed only to be interviewed anonymously. Mention of an organization's name in this Article does not imply its participation in a CLP interview.

SaaS, PaaS or IaaS *services* to users, where providers could include integrators.[9] We do not analyze end-user software licenses relating to cloud infrastructure or applications running on cloud infrastructure. In cloud computing, users obtain services, which may include rights to run software owned by the provider (or licensed by it from the rights owner for the purpose of providing services to third parties who, in using the provider's services, run such software in the cloud). However, cloud users procure primarily services, not licenses.

The possibility of chains of services and providers (not always known to users)[10] means users may rely on multiple parties, with multiple possible points of failure. Cloud users generally also depend on internet connectivity—usually involving contracts with telecommunications providers.[11] We do not discuss such contracts, contracts for consultancy or advisory services for users' adoption of cloud computing (sometimes forming part of a larger package), or contracts for supporting services for, or working with, the primary cloud service.

Also, while cloud users may have their own individual end users (e.g., employees or customers using the service procured) we focus only on the cloud user's relationship with its cloud provider, not its own end users. The sole exception involves integrators, where we discuss wholesale contracts with their providers, where they are users, or their end user customers, where they are providers.

II. CLOUD PROVIDERS' PERSPECTIVE

The starting point for cloud contracts is usually the providers' standard terms and conditions, which are provider-favorable and, generally, are designed for high-volume, low-cost, standard, commoditized services on shared multi-tenant infrastructure. However, as many providers' standard terms are not suitable to accommodate enterprise users' requirements, cloud users have sought

9. Several entities may be involved in providing a single cloud service, including suppliers of hardware, software, and data center services. There may be chains of contracts between them. Contractual requirements may vary with the cloud "stack" component under consideration. *See* Bradshaw et al., *supra* note 2, at 11; W. Kuan Hon, Julia Hörnle & Christopher Millard, *Data Protection Jurisdiction and Cloud Computing—When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing Part 3*, 26 INT'L REV. L. COMPUTER & TECH. (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240.

10. *See* W. Kuan Hon, Christopher Millard & Ian Walden, *Who is Responsible for 'Personal Data' in Cloud Computing?—The Cloud of Computing Part 2*, 2 INT'L DATA PRIVACY L. 3 (2012), *available at* http://idpl.oxfordjournals.org/content/2/1/3; W. Kuan Hon & Christopher Millard, *Data Export in Cloud Computing—How can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing Part 4*, 9 SCRIPT-ED 25 (2012), *available at* http://script-ed.org/wp-content/uploads/2012/04/hon.pdf.

11. Indeed, some sources felt that the biggest issue for cloud, although not discussed much, was responsibility for the underlying network, and who takes the risk of its failure (sometimes, integrators).

changes to make the terms more balanced and appropriate to their own circumstances. It appears that there has been some movement in this direction, particularly for large users. Nevertheless, our research indicates that some providers' negotiations are very process-driven, particularly at the lower price end of the market, where providers seemed unable or unwilling to accommodate differences such as corporate structures entailing (for users) separate localized contracts for non-United States affiliates.

III. CLOUD USERS' PERSPECTIVE

Before discussing contract terms changes that users have requested, and areas where they have succeeded, we first discuss why they may want changes, and factors that may influence whether providers accede. Drivers for users to seek changes to providers' standard terms may be internal or external. Internal reasons obviously include commercial issues such as required high service levels for mission-critical services, and allocation of risk between user and provider (particularly provider liability). External drivers are chiefly regulatory, namely, the need to comply with laws and regulations, including regulatory action. However, other external drivers are possible, such as insurers, whose role in the evolution of the cloud market is likely to increase.[12] Insurers may influence terms by, for example, insisting on certain certifications before agreeing to insure services—although according to one specialist United Kingdom cloud insurer, more providers than users were insuring, mainly for liability and errors and omissions.

Factors affecting development of cloud contract terms will be led by both demand and supply. More customer-friendly terms are being demanded by large users such as government, and being offered or agreed by integrators, smaller or specialist providers, and market entrants, thus making contract terms a source of competitive advantage for providers. As such, we believe that standard terms will improve from users' perspective as the market develops further. Our findings tie in with a survey for the Cloud Industry Forum of 450 senior information technology and business decision makers in enterprises, small and medium-sized businesses, and public sector organizations, published in early 2011. This found that, while forty-eight percent of organizations polled were already using cloud, only fifty-two percent of those (particularly larger organizations) had negotiated their contracts, with forty-five percent stating that they had no opportunity to negotiate (click-through terms, discussed below). In other words, according to that survey, about half of such users' cloud contracts were negotiated.[13]

---

12. Currently, many insurers view cloud as a form of outsourcing, which may already be within the scope of policies covering outsourcing.

13. Cloud Industry Forum, *Cloud UK: Paper Three – Contracting Cloud Services: A*

A. *Risk Management, Internal Controls, Governance, and Awareness: The Click-Through "Trap"?*

Many providers' roots lie in click-through web services offered to consumers or small and medium-sized enterprises, where users are presented with providers' standard contract terms, and "click through" to accept the terms, without any opportunity for negotiation. With many services, the only additional step is for users to enter credit card details, whereupon they may start using the service immediately. This history seems reflected in contractual terms and sign-up procedures for cloud services generally. Cloud providers' contracts are often "click-through," as the nature of cloud services enables use of a click-through consumer-based distribution model, and some providers deliberately choose that model for cloud. Other providers maintain generic click-through online terms for "self-service" customer-managed services, aimed at smaller or trial users, but offer (possibly regionalized) framework or master agreements for larger users enabling specific services to be purchased online.

For providers, click-through can eliminate negotiation costs and may reduce legal liabilities and other risks.[14] Some users noted that some providers, even large ones, did not have sufficient in-house legal resources to deal with users' requests to change terms, which might be another reason why they refuse to negotiate. One IaaS provider noted that they had never had a customer try to negotiate its standard click-through terms. Another provider was considering moving to 'click-through only' specifically to avoid the cost and time of negotiating terms.

However, the "click-through" model poses risks for users, such as fostering a bypass, sometimes deliberate, of institutional procurement processes.[15] A

Guide to Best Practices (2011) [hereinafter *CIF3*], *available at* http://www.cloudindustryforum.org/downloads/whitepapers/cif-white-paper-1-2011-cloud-uk-adoption-and-trends.pdf.

14. However, non-negotiated standard terms may be unenforceable in some circumstances, even against businesses; *see* Unfair Contract Terms Act, 1977, c. 50 (U.K.). A future CLP article will discuss consumer protection law issues.

15. Possibly encouraged by some traditional in-house information technology functions' perceived lack of responsiveness, coupled with the desire of those concerned to deploy quickly without the perceived delays of dealing with internal information technology, security or legal functions. *See, e.g.*, David Linthicum, *3 Reasons Cloud App Development is Taking Off*, INFOWORLD (Oct. 20, 2012), http://www.infoworld.com/d/cloud-computing/3-reasons-cloud-app-development-taking-176439 ("Employees frustrated with the wait for corporate IT [this is a direct quote, so reinstate the abbreviation here?] to solve a business problem simply hire their own developers and use PaaS as a cheap way to get their applications built, tested, and deployed."). Perhaps also, users are habituated to "clicking through" to agree terms automatically, from websites' standard processes for online sales of consumer products or services. In this sense, click-through for cloud contracts reflects the influence of

survey in 2010 found that fifty percent of information technology and information technology security specialists (forty-four percent in Europe) were not aware of all cloud computing resources deployed in their organizations.[16] Of decision makers accountable for cloud services, a "surprisingly high" number responded "don't know" to several key questions in a 2011 survey.[17]

While click-through may enable more efficient and flexible provisioning of information technology services, users' risk exposures may be affected. As certain German data protection regulators noted,[18] click-through's speed and ease means some customers may be tempted to accept providers' standard terms online, in order to start using the desired service quickly, without considering fully the nature or effect of those terms, or going through their organization's standard procurement procedures (such as legal or data protection review or security or other risk assessments).

It is not unknown for users to discover their employees had subscribed to cloud services on providers' standard terms, and then attempt to negotiate more acceptable terms. One SaaS provider noted that sometimes users were unaware of other internal departments using its service; only when the user's information technology department discovered the position was the user able to consolidate services. Some cloud services were even being used without any written contract, whether because they were free or being trialed on a pilot or test basis.[19]

Perhaps some employees bypass internal procurement procedures in situations where services are free of charge, at least for basic services. However, "free of charge" or "low cost" does not necessarily mean "free of risk" or "low risk." Legal, regulatory or reputational risks may exist. This is particularly true if data involved are not "fake" test data but constitute "real" data, perhaps even confidential or personal data. Furthermore, organizations may still be charged for essential supporting services or "extras" beyond the "free" component, for

---

consumer distribution models.

16. Larry Ponemon, PONEMON INST., SECURITY OF CLOUD COMPUTING USERS: A STUDY OF PRACTITIONERS IN THE U.S. AND EUROPE 6 fig.7 (2010), *available at* http://www.ca.com/~/media/Files/IndustryResearch/security-cloud-computing-users_235659.pdf

17. *CIF3*, *supra* note 13, at 3-4 (polling some 450 decision makers).

18. DER ARBEITSKREISE TECHNIK UND MEDIEN DER KONFERENZ DER DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER, ORIENTIERUNGSHILFE – CLOUD COMPUTING (2011) § 4.1.2 (Ger.), *available at* http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf [hereinafter DATENSCHUTZBEAUFTRAGTEN].

19. *See, e.g.*, Letter from Chelsea and Westminster Hosp., Aug. 3, 2011 (on file with author). In response to a freedom of information request regarding Chelsea and Westminster Hospital's tests of cloud computing for healthcare involving Flexiant, the Data Capture and Auto Identification Reference Project (DACAR) based at Chelsea and Westminster Hospital, and Edinburgh Napier University, the hospital replied, "There is no contractual agreement between Flexiant and Chelsea and Westminster Hospital Foundation Trust at this time."

example Postini spam filtering for Google Apps SaaS.

Even where contracts were negotiated, some users' lawyers commented that their involvement had not been sought at an early enough stage to influence negotiations: "Business or procurement people negotiate without lawyers in the room; eventually the contract gets to legal staff, but not soon enough!" It is difficult for a user's lawyers to change contract terms when they are told that the contract has already been agreed upon, the service is going live shortly, and to "just do a quick review."

Not involving lawyers in transactions from the outset may, in some organizations, be prevalent in relation to other types of contracts too. But while attempts to circumvent "the lawyers say 'no'" may speed up deals, they may also expose organizations to liability and other legal risks. Sometimes, users' lawyers were even asked to draft or review cloud contracts without being told the service's nature or purpose. This also poses risks: IaaS is quite different from SaaS, while a SaaS data storage service for managing an individual customer's personal data should be approached differently from a service intended only to record meteorological readings.

Providers have greater control in the cloud, particularly with SaaS, with correspondingly reduced user control, as illustrated by publicity regarding limitations in Microsoft Office 365's "P" Plan, where users were restricted in how many e-mails they could receive in twenty-four hours.[20] This provider constraint, which would not be possible with traditional e-mail applications installed on internal servers, illustrates the need for users to scrutinize contractual terms before signing up. However, procedurally, sometimes providers make terms available only late in the sign-up process, which may make it harder for users to compare different offerings at an early stage.

The above suggests that there may be internal governance and cultural issues which some organizations need to consider and address as part of their overall risk management strategy, both internally and in relations with providers. Scrutiny of procedures and practices, including training, may be in order. Otherwise, some organizations may find themselves committed[21] to cloud contracts on terms unfavorable to them, exposing them to possible legal risk, including breach of legal or regulatory obligations which may subject them to civil or even criminal liability.

Some users, such as News International, flag credit card charges by employees signing up for Amazon Web Services IaaS and the like, partly to secure

---

20. Ed Bott, *Small Businesses, Beware the Office 365 Fine Print*, ZDNET (Oct. 21, 2011, 3:00 AM GMT), http://www.zdnet.com/blog/bott/small-businesses-beware-the-office-365-fine-print/4151.

21. Assuming the employees concerned at least have ostensible authority to bind the organization, which seems likely.

better block pricing.[22] However such flagging may not be possible with sign-ups for free services. Another user, which is also a provider, has a policy banning employees from clicking through on standard term cloud contracts.

There also seems to be an educational issue for users' lawyers. Some providers' lawyers pointed out that users' lawyers sometimes raised points on providers' standard contract terms for the "wrong reasons," such as "going to town" to justify their fees! The most important reason was lack of understanding amongst such users' lawyers about cloud computing and what the user was buying. Many users' lawyers' approached cloud contracts as software licenses or technology acquisitions, rather than as contracts for services. Others treated them as classic information technology outsourcing, without taking proper account of cloud computing's unique features. One SaaS provider found the largest users negotiated the least, perhaps because the deal was relatively small for them, or perhaps because they better understood the nature of SaaS, so they did not seek terms inappropriate to cloud computing. However, it must be said that users' lawyers have also suggested that some providers' terms are too software license-orientated, and there is room for them to be more cloud-appropriate. Indeed, our sources considered that, even in the information technology industry, many intermediaries have been treating cloud computing as a supply of products or licenses rather than services. All this seems to indicate the relative immaturity of the market.

While not the key focus of this Article, pre-contractual due diligence should not be overlooked. This may include security,[23] disaster recovery, data retention and return of data on exit (including data formats), and exit strategies.[24] We discuss contractual provisions on those issues below.

B. *To Negotiate, or Not to Negotiate?*

Users may decide that, for small initial pilots or tests of moving specific workloads or processes to the cloud, the time and costs of negotiating providers' standard terms are not worthwhile. For example, the Alpha.gov.uk prototype, for a single site for United Kingdom government online services, was based on Amazon's IaaS, using Amazon's standard terms on a click-through

---

22. Paul Cheesbrough, Presentation at Amazon Summit: AWS Use at News International (June 14, 2011), *available at* http://plugyourbrand.com/AWS_Summit_2011/#trail_head/presentations.

23. For pre-contractual security checks (not limited to data protection), European Union data protection authorities have suggested European Network and Info. Sec. Agency, *Cloud Computing: Information Assurance Framework* (Nov. 2009).

24. However, it seems only 45% of United Kingdom cloud users had a plan to migrate to another provider on any service interruption or termination (with 12% responding "don't know"). Similarly, only 45% of integrators had such a plan. CIF3, *supra* note 13, at 9.

basis.[25] Similarly, Warwickshire County Council's pilot of Google Apps[26] commenced in late 2011, on Google's standard terms. Only when considering full migration of the relevant function, or processing of "real" data, particularly personal data, might such users then scrutinize contract terms.

However, users may not be able to negotiate providers' terms. As with any commercial agreement, much depends on relative bargaining power. Large providers generally decline any changes to their standard terms, insisting their services are only on a "take it or leave it" basis—even when requested by large users, such as integrators. Some users have had to "take it," negotiating only commercial terms (price, payment frequency, perhaps availability levels), because "we needed them more than they needed us." Other users have walked away.

Some users appear to accept the general inability to negotiate providers' standard terms and agree to those terms notwithstanding.[27] Nevertheless, even large providers have departed from their standard terms to secure deals they perceive to be sufficiently worthwhile in terms of financial, strategic or reputational "trophy" value. For example, there was publicity about Google's deals to provide Google Apps SaaS to the City of Los Angeles,[28] and more recently to Cambridge University.[29] Some smaller SaaS providers consider requests to change standard terms from larger customers, such as those expected to pay more than a certain amount annually.

Generally, bigger users, particularly from regulated industries, try to negotiate more. Indeed, some go further, insisting on cloud contracts being on *their* own standard information technology services or outsourcing terms, on a "take it or leave it" basis. Such users mainly comprise government bodies and financial institutions. Partly they may have more purchasing power, but also their internal procedures may make it difficult and time-consuming to contract on terms other than their own (for example, banks may require director sign-off for changes to their standard terms). To secure such users' business quickly, some providers may accept the user's terms, although some terms may not suit

---

25. Government Digital Service response to freedom of information request (Dec. 22, 2011) (on file with author).

26. Kathleen Hall, *Warwickshire County Council Signs Google to Pilot G-Cloud E-mail Service*, COMPUTERWEEKLY.COM (Sept. 19, 2011, 5:00 AM), http://www.computerweekly.com/news/2240105636/Warwickshire-County-Council-signs-Google-to-pilot-G-Cloud-e-mail-service.

27. *See CIF3*, *supra* note 13, at 4-5.

28. Reportedly, however, there have been problems. *See, e.g.*, Jon Brodkin, *Google Apps Hasn't Met LAPD's Security Requirements, City Demands Refund*, ARS TECHNICA (Oct. 20, 2011, 8:09 AM), http://arstechnica.com/business/news/2011/10/google-apps-hasnt-met-lapds-security-requirements-city-demands-refund.ars.

29. Google Apps Education Edition Agreement, UNIVERSITY OF CAMBRIDGE, http://www.ucs.cam.ac.uk/googleapps/google-apps-cambridge-contract.pdf (last visited May 9, 2012).

cloud services.[30]

Thus, both providers and large users want to contract on their own standard terms, although generally neither set of terms seems optimal for cloud contracting arrangements.

C. *Role of Integrators*

Of growing significance in cloud is the information technology channel: termed by the Cloud Industry Forum "Reseller, Service Provider and Outsourcer," comprising information technology consultancies,[31] managed services providers, systems integrators, specialist resellers, technical value-added resellers, information technology outsourcers, distributors and volume resellers, and information technology retailers. We use "integrator" to mean "reseller, service provider or outsourcer."

Integrators contract with both end users and providers, unless their end users contract directly with providers.[32] Therefore, in many ways, integrators are like providers who use other providers to offer services to their own end users. Integrators are potentially very large users of IaaS or PaaS, based on which they provide services (particularly SaaS) to their end users. Integrators may also provide cloud services on infrastructure they control, such as IBM's Smart Enterprise Cloud, or HP's Enterprise Cloud which includes SaaS and IaaS. They also offer customized cloud services, particularly private or hybrid cloud.

According to our research, integrators are better able than end users to negotiate improved terms with providers.[33] This may be because integrators may have ongoing relationships with providers, and perhaps better bargaining position with larger business volumes, as an integrator may use the same provider

---

30. W. Kuan Hon, et al., *UK G-Cloud V1 and the Impact on Cloud Contracts – Part I*, 17 COMM. L. 78 (2012); W. Kuan Hon, et al., *UK G-Cloud V1 and the Impact on Cloud Contracts – Part II*, 17 COMM. L. __ (forthcoming 2013).

31. Which may include advice on migration to cloud, building cloud hardware or software (on clients' or third party infrastructure), support or training.

32. Forty-three percent of United Kingdom cloud services resellers contracted directly with end user customers, 12% required customers to contract with providers (typically on commission), 28% offered a mix dependent on solutions required. 48% offered back-to-back terms between supplier and customer. *CIF3*, *supra* note 13, at 5.

33. Cloud Industry Forum findings were similar: a (provider-favorable) right for providers to change contracts unilaterally by posting a new version online was imposed in contracts with 32% of users, but only 19% of integrators who were resellers. *See CIF3*, *supra* note 13, at 5. Despite their seemingly better bargaining position, however, only 40% of integrators (compared to 52% of end users) were reported to have "consciously negotiated" contracts with providers (since presumably those surveyed were aware whether their organization had negotiated). *Id.* at 4; Cloud Industry Forum, *Cloud UK: Paper Two – The Impact Upon the IT Supply Chain* 12 (2011) [hereinafter *CIF2*], *available at* http://www.cloudindustryforum.org /downloads/whitepapers/cif-white-paper-2-2011-cloud-uk-impact-upon-the-it-supply-chain.pdf.

to service multiple customers. However, with large providers, we found even global integrators had difficulty obtaining the changes they or their customers needed for data protection or security purposes.

We found some end users contracted with integrators, rather than with providers, because some integrators were prepared to give more contractual assurances than providers. For instance, some interviewees mentioned users contracting with integrators for Office 365, rather than using Office 365 on Microsoft's infrastructure, enabling users to obtain from integrators contractual assurances they could not have obtained from Microsoft, in terms of liability or liability caps, service levels and credits, support, and backups.

However, if in such cases the integrator's contract with the provider is not truly "back to back," integrators bear the risks of any mismatch in obligations and liabilities. "If we use a cloud service, as a systems integrator we have to be very careful about what the customer requires, because we might not be able to get that from the cloud service provider," one stated. "We're taking a big slice of the risk pie," another noted. In many cases, integrators make a calculated decision to take that risk, to gain or retain users' business by better meeting their needs. They consider risks in some respects may be spread over end users, and take a view on aggregated risk. Such a position may also receive some encouragement from the insurance market.[34]

However, integrators' greater willingness to assume risk is not unlimited. Integrators noted that where users insisted on a particular provider, if the integrator could not persuade the provider to amend standard terms to meet customer requirements, it had to make that position clear to the customer, and sometimes leave the customer to contract directly with the provider. Hence, while some integrators do not wish to invest in infrastructure, others already are, or are considering, providing cloud services on infrastructure they control, in order to offer users such as banks the assurances they need while being able to manage their own exposure better.

Integrators may also offer mixed cloud and non-cloud services, particularly to large users, where cloud computing is just one service forming part of a larger package of services or "whole business" deal, including for example internet connectivity or consultancy services. Similarly, customers may seek SaaS management or monitoring tools within more traditional large outsourcing deals. Contracts for such deals will obviously reflect the cloud component's relatively minor position.

---

34. *See, e.g., The Cloud Risk Framework: Informing Decisions About Moving to the Cloud*, MARSH & MCLENNAN COMPANIES (2012), http://f.datasrvr.com/fr1/812/29871/3424_MA12-11623_Cloud_Computing_Frmwk_UK_04-2012_final_nocrps.pdf.

D. *Other Relevant Factors*

The extent to which users may need to negotiate contracts will obviously depend on how much relative control the particular system's design affords users and providers over users' applications or data, and how "customer friendly" a provider's standard terms are. With paid-for services, providers are generally more willing to accept liability (or greater liability), and agree other user-requested commitments or measures, than with free services.[35] The more providers are paid, the more they are willing to concede. Market factors also play their part, with a global user noting that one large provider was more flexible than others because it was trying to "catch up" in the cloud space, and indeed was more flexible on cloud than on other types of contracts.

IV. CLOUD CONTRACT TERMS: DETAILED ANALYSIS

A. *Liability: Exclusion, Limits and Remedies for Breach of Warranties and Indemnities*

Providers' exclusion of liability, particularly for outages and data loss, was generally the biggest issue for users.[36] Providers try to exclude liability altogether,[37] or restrict liability as much as possible,[38] because they provide commoditized services: understandably, providers may not wish to be exposed to say $100 million of liability for a deal worth $1 million; and unlimited liability could put smaller providers out of business.

According to our research, providers state liability is non-negotiable, and "everyone else accepts it." Even large users had difficulty getting providers to accept any monetary liability, with one global user stating that generally it "had to lump it," and another saying, "they won't move." Refusal to accept any liability was cited as a "deal breaker" by several users. Although liability exclusion is more widespread and more acceptable under United States jurisdictions, some United States users still refused to deal with some providers who excluded liability.

However, some global users negotiated successfully for provider liability. This might be more common where cloud services formed part of a larger deal,

---

35. Bradshaw et al., *supra* note 2.

36. In the Cloud Industry Forum survey, providers excluded liability for data loss for 34% of United Kingdom cloud users, accepting capped liability for data loss and breach of contract for 54%. With integrators, providers accepted more liability: 20% of providers excluded liability, 31% agreed capped liability; and 27% accepted full liability. *CIF3*, *supra* note 13.

37. Bradshaw et al., *supra* note 2.

38. For example, in the United Kingdom, liability cannot be excluded for negligence causing death or personal injury.

such as telecommunications. If liability was agreed, it was almost invariably accepted only in limited circumstances, restricted to narrowly-defined types of damage: typically, "direct" losses only, with no liability for indirect or consequential losses. Where liability was accepted for "direct losses," that term's definition might be much discussed.

Some users, particularly those who could insist on their own standard terms, such as financial institutions or government, secured unlimited liability for defined types of breach or loss, notably breach of confidentiality, privacy or data protection laws, or breach of regulatory or security requirements such as breaches giving rise to regulatory fines. One integrator commented, "For privacy breaches there is no cap that people will agree [to] that would be sufficient."

However, more commonly, liability was capped, sometimes with different caps for different types of losses, and often limited by reference to amounts paid by the user in total or over a period like a year, such as 100% or 125% of six months' fees.[39] Some providers would agree a higher percentage or longer period of fees for certain deals, such as where fees were paid up front.[40] Users who could impose their own terms might cap liability at a higher proportion, say 150% of charges paid over the last year.

Some telecommunications providers appeared more willing to accept some liability. This may be because they control internet connections to users and therefore have greater control regarding connectivity and service availability. Smaller providers also seemed more flexible, with one enterprise-oriented SaaS provider accepting liability for outages as standard if caused by internet connectivity failures at its data centers, whereas many large providers would not accept any monetary liability for outages however caused. As previously mentioned, some integrators also seemed more willing to accept liability, so that, for example, a global user contracted with an integrator who accepted liability for data loss, when the provider would not accept liability.

Conversely, providers have argued that, in trying to remove or reduce liability exclusions and limitations or increase service levels for commoditized services, customers want to have their cake and eat it too—seeking the cheapest services while requesting the highest levels of assurances. More technologically-sophisticated users stated that they arranged their own backups, for example to their own servers, while a provider noted that users were beginning to understand that they cannot expect much provider liability for low cost services.

Some SaaS providers emphasized that they provide services, rather than li-

---

39. Interestingly, an integrator commented that some providers who indicated willingness to offer capped liability subsequently reverted to total liability exclusion. Also, one SaaS provider observed that its liability ceiling was not negotiated as often as one might think, although it was questioned more in higher value deals.

40. Cloud Industry Forum recommends providers consider offering higher caps for higher fees. *See CIF3*, *supra* note 13, at 13.

censing software, and preferred not to include any contractual software licenses, to avoid associated risks. With open source software, providers would exclude liability for intellectual property rights infringement. Many users wanted providers to warrant that intellectual property rights relating to application software used in the cloud were the provider's and that the service did not infringe third party rights, with appropriate indemnities. This might not be possible where providers licensed applications from third parties to offer SaaS services. To address third-party intellectual property rights, for example intellectual property rights belonging to providers' own suppliers, some users requested copies of third party indemnities to providers and sought back-to-back indemnities from providers. The indemnity's scope might require scrutiny for suitability. For example, one global provider, whose SaaS service included the supply of certain content, limited its liability only to copyright infringement, excluding patent-related infringements. Generally, as with other kinds of liability, intellectual property rights indemnities were limited to direct losses only, and capped. One global user declined to deal with a SaaS provider who restricted intellectual property rights indemnities to certain countries' intellectual property rights only, and limited the amount and losses covered.

When considering provider liability, contractual provisions are not the only factor. Several sources pointed out that providers offering unlimited liability may not be creditworthy should losses arise, but users may find it easier to put forward to directors contracts where providers assume rather than exclude liability. Too much focus on contractual terms rather than, for example, financial standing may thus be too narrow for risk management purposes.

B. *Resilience, Availability, Performance and Service Levels*

1. *Data integrity, resilience and business continuity*

A common theme was business continuity and disaster recovery, i.e., how to ensure integrity and availability of cloud data and applications. One user noted, "Providers tend to say cloud is very redundant, fault-tolerant, there's no need for disaster recovery—but there is."

Many providers take two or three backups of data in practice, perhaps even onto backup tapes, although they may not commit contractually to doing so. While some will undertake to make the necessary number of backups, most will not warrant data integrity, or accept liability for data loss. Where a SaaS service included the supply of certain data, liability was limited to replacing any lost data.

Confidentiality provisions may result in liability upon any data security breach, but not for data loss or corruption, as unauthorized access to user data may result in confidentiality breaches, but data loss or corruption may not. Therefore, specific warranties (with liability) in relation to data loss or corruption may be important in addition. Some global users have secured such war-

ranties, for example unlimited liability for data loss or corruption, for one financial institution, and even monetary compensation for data loss including recovery costs, for another global user.

One non-European telecommunications provider undertakes to backup data and guarantees their integrity, commenting that Amazon did not because its charges are low. Many providers, including Amazon, offer backup as a separate service: if the user pays extra, the provider undertakes to make backups, and assumes liability for the integrity of backups and data loss.[41]

Providers such as Amazon stress that cloud involves shared responsibility: both users and providers have responsibility for data integrity, backup and security, and allocation of responsibilities and risks needs careful consideration.[42] Users generally have more control with IaaS or PaaS than with SaaS, because IaaS users instantiate or terminate virtual servers and choose what to install on those servers, such as firewalls, anti-malware and other security measures; and users decide what applications they wish to install and host on IaaS or PaaS, such applications often being user-developed and therefore user-controlled. In contrast, SaaS users use standardized applications, provided by SaaS providers in environments which users cannot control, relying on providers to secure applications as well as environments. The users we interviewed who were more technically aware, such as technology businesses or integrators, tended to recognize the need to implement their own backup strategy, rather than expecting providers to backup as part of their basic service. An integrator using cloud to provide SaaS services to its own users implemented its own extensive disaster recovery procedures, backing up or failing over to the same or separate data centers or another provider, depending on end users' risk tolerance.

2. *Service levels, service credits*

There were different approaches to service level agreements (SLAs), i.e. commitments on availability levels and performance. This was probably because availability levels are often quite high, and capacities, performance, and service levels are normally negotiable commercial issues varying with user requirements, rather than legal issues—for instance, guaranteeing different service levels at different prices.[43]

---

41. One enterprise-oriented SaaS provider noted that force majeure was often raised in relation to provider liability, depending on whether it was required to make backups, and whether the force majeure incident also affected the backup.

42. *See, e.g.,* AMAZON *Web Services: Overview of Security Processes,* AMAZON.COM (May 2011), http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf.

43. Cloud Industry Forum recommends that providers document management systems, processes and resources for consistent service delivery, specify whether users may audit business continuity or disaster recovery processes, and publish average availability times. *See* CIF3, *supra* note 13, at 12.

Standards are still lacking, making it difficult for users to compare different services. In large deals, methods for measuring service levels were often debated, with users wanting numerous key performance indicators, although at the low end providers stipulate the metrics, generally not exceeding five or ten key performance indicators.

Providers justify refusing to negotiate service levels on the basis that they provide commoditized services. One enterprise-oriented SaaS provider stated it did not even offer SLAs. Very few of its users, about 0.2%, had requested SLAs; fewer still wanted as high as 99.7% uptime. Possibly this was because it had designed its service for very high uptime levels, and published information on historic service levels.

If availability, reliability and performance are vital, such as with mission-critical applications or real time services, users may consider issues such as how the load on providers' infrastructure from other users can affect the user's application performance; how well the service handles peak spikes; how sufficient robustness is ensured, and so on.[44] One issue which seemingly has not seen much discussion is the risk of additional users adversely affecting the service, because capacity in the cloud is not in fact unlimited. This may result in SLA breaches, yet reportedly users generally did not try to restrict how quickly providers added new users or how much capacity they could offer new users.

Users with mission-critical applications may accordingly seek higher availability levels, warranties regarding response times, undertakings not to terminate services without notification and consent, longer prior notification of proposed maintenance downtime, perhaps even notification of usage exceeding agreed limits (to allow the user to investigate and manage the situation), rather than immediately throttling usage and slowing performance without consulting users. However, providers are unlikely to warrant latency (response time), unless perhaps they control the network, such as some telecommunications providers or integrators, who for a price will warrant low latencies. One provider considered that what users truly want, but providers did not offer, was guaranteed application performance, for example X simultaneous users with maximum Y response time; it believed there would be increasing focus on application performance management and monitoring.

Users may also consider how and how long it takes to restore data from backup if systems go down or data are lost. One integrator commented that providers' response time requirements were "nothing like what clients insist upon."[45] The time lag varies with providers, from seconds for some business-oriented services (which accordingly charge more), to days.

SLAs are often referenced by linking to providers' published website de-

---

44. Bradshaw et al., *supra* note 2, at § 4.19.

45. Cloud Industry Forum recommends providers should specify protocols and service level agreements for restoring data from backups. *CIF3*, *supra* note 13, at 11.

tails, which providers may amend, thus putting the onus on users to monitor providers' sites for changes.[46] As this is burdensome, some users have required prior notification of impending SLA changes.

For SLA breaches, remedies are normally excluded except as specifically provided. Providers generally exclude any remedies other than service credits, even for total service failures, although some allow optional termination if SLAs fall below a certain percentage, and may even accept liability for some monetary compensation if (but only if) terminated. Standard terms generally circumscribe the circumstances when service credits are given; for example, they may give credits only for failures arising from matters under the provider's control, or only if credits are claimed within a certain period. One global user, who uses cloud computing to provide real-time services to end users, did not insist on performance warranties or even service credits, as any outage would be highly detrimental to its reputation so even monetary compensation would probably be inadequate, and service credits were difficult to quantify. Therefore it decided simply to accept standard SLAs.

Even where service levels are non-negotiable, service credits for SLA breaches may be. However, while preferring service credits, some providers do offer benchmarked "money back" rebates or monetary compensation.

3. *Transparency*

Our research indicated that there are two main ways in which availability data is provided to users: users may monitor availability themselves, or providers may provide the information to users, such as specific webpages which are kept updated, and which users may check.

A global user stated that if the contract included SLAs, it would further require reporting of statistics. Similarly, a non-European telecom provider mentioned that it offered SLAs according to users' requests, and would commit to keeping users informed proactively within certain boundaries ("tell them before they tell us").

Where availability was critical, users might monitor the service or application themselves, for example for failure of virtual machine ("VM") instances, using the provider's tools or (as many providers do not allow user access to their tools) public tools or the user's own tools. However, too much user monitoring may itself affect application performance (and increase bandwidth usage charges). After assessing the impact of monitoring, one large user was persuaded not to monitor. One global user also pointed out that providers' usage monitoring for billing purposes may affect service performance. Therefore, for services where near real-time response times are critical, some users sought rights

46. Bradshaw et al., *supra* note 2.

to require providers to pause or stop monitoring if materially detrimental to performance. One integrator stated that it usually monitored charges itself, depending on the setup of the service.

It seems providers generally could do more to improve transparency regarding availability and service levels by providing such data to users proactively. Illustrating that greater transparency is possible technically, trust.salesforce.com and Microsoft Dynamics CRM were cited as services enabling users to check, even in real time, data on performance and availability of services. Such transparency may involve technical changes and costs for providers. Generally it is providers with large enterprise customer bases who are providing such data for users.

4. *Users' liability*

Another issue is users' liability to providers, particularly where users employ cloud computing to deliver services to their end users. Unsurprisingly, users who could negotiate their contracts would not accept liability to providers. One global user declined to contract with a provider who required such liability.

Cloud users, not having control over their own end users' actions, also declined to indemnify providers for such actions, even if constituting breaches of providers' terms, even if causing loss to the provider. A compromise was for providers to terminate or suspend the service, with sufficient prior notice for users to investigate and terminate the culprit's account if necessary. Such users also ensured that their contracts with end users allowed termination for misconduct, with indemnities from end users.

C. *Regulatory Issues*

Generally, providers' role regarding their users' compliance obligations still seems not well defined, understood or accommodated by providers. A common theme was that many providers, in standard terms or even in negotiations, would not take into account that users have regulatory or other legal obligations and may need to demonstrate compliance to regulators. Some users expressed frustration at providers' lack of empathy with their compliance obligations, especially in Europe. For some users, the solution was to use cloud computing only in less highly regulated jurisdictions, such as some Asian countries. Integrators are in an interesting position, being "caught in the middle," as the compliance responsibilities are generally not theirs but their end users'.

It seems some providers simply have not considered regulatory requirements' impact on their terms.[47] Several users noted this. One discovered, after

47. To some extent, this may reflect some users' lack of focus on regulatory or legal

protracted negotiations, that a global provider had never conducted a regulatory review of its own services or terms, let alone of its contract with its own sub-provider. Reportedly some users had, for cost-saving reasons, decided to use cloud despite inadequate contract terms, "taking a view" on regulators discovering and enforcing any non-compliance. However, one integrator commented that, although providers refused to negotiate privacy and security issues, when users refused to sign, some would agree changes.

Regulatory issues varied with jurisdiction; more issues reportedly arose with, say Germany or France, than the United Kingdom. But with European users generally, and users outside government and financial sectors, data protection laws were the most commonly-cited regulatory issue. This seems unsurprising, as data protection law is "horizontal" rather than "vertical," meaning that it regulates all sectors, and controllers of personal data remain responsible if processing data in the cloud. Financial sector regulation was another key regulatory issue.

Data location and data confidentiality were the top data protection law concerns, followed by data processor and transfer agreements and the role of sub-providers, while for financial institutions the biggest issues were security requirements and audit rights.

1. *Data location and data export*

Users were not concerned about colocation[48] within a third party's data center, so much as geographical location of data centers. Many users were concerned about the location of data center(s) employed by their providers, particularly if using data centers outside the European Economic Area. Conversely, other users specifically wanted data kept offshore, such as in the Channel Islands, but never in the United States.

The Data Protection Directive prohibits transfers of personal data outside the European Economic Area except in specified circumstances, such as when recipients are certified under the United States Safe Harbor scheme, or where using standard model clauses or binding corporate rules.[49] This prohibition is significant. Global users have refused to contract with providers who declined to include terms to comply with the Data Protection Directive's international

---

issues when procuring cloud services. *See supra* Part III.B; *see also* Edward F. Moltzen, *Analysis: Dropbox Carries Risks For SMBs*, *CRN*, (Nov. 4, 2011), http://www.crn.com/news/cloud/231902380/analysis-dropbox-carries-risks-for-smbs.htm (noting that the then new Dropbox for Teams cloud storage service did not meet Payment Card Industry requirements or the United States Health Insurance Portability and Accountability Act or Sarbanes-Oxley Act; Dropbox responded that customers who beta-tested the service prior to launch were concerned with collaboration and ease-of-sharing, not the cited requirements or laws).

48. Namely, sharing hardware or software with other customers in the same location.

49. Hon et al., *Data Export in Cloud Computing*, *supra* note 10, at 30-31, 41-47.

transfers requirements.

The Cloud Industry Forum recommends providers offering European Economic Area-only locations should inform users accordingly. Indeed, European Economic Area users might consider this a selling point. It also recommends providers should disclose all data center locations, including those used for backups, and whether data may be transferred outside the European Economic Area.[50] However, some providers will not disclose data center locations.

Users have sought, and sometimes obtained, warranties or undertakings that all data centers used for their data were in the European Union and European Economic Area or that data were located only within the European Union. One United Kingdom-based global user stated that, although it did not process personal data in the cloud, it still required its global provider to confine processing to European Union data centers, and, should it nevertheless transfer data to the United States, it must be certified under Safe Harbor and comply with its principles.

Some services allow users to choose locations of data centers used to process users' data, e.g., European Union-only,[51] while providers are increasingly offering, albeit with exceptions, to restrict data to users' chosen locations as standard.[52]

Verifying that data are actually processed in the data centers claimed by providers is difficult, technically.[53] One provider noted that some providers were misleadingly labeling servers as "EU" when they could process data elsewhere. One public sector user felt warranties of United Kingdom-only data location could be untrue, citing a hosted services provider who stated that data storage was limited to the United Kingdom, but whose IP address indicated a United States location.[54]

Users may need location information for reasons other than the restriction on transferring personal data outside the European Economic Area. The Data Protection Directive requires controllers to choose processors providing "sufficient guarantees" regarding security measures for processing, and to ensure compliance with those measures. This may be difficult without more transpar-

---

50. *CIF3*, *supra* note 13, at 11.

51. Hon et al., *Data Export in Cloud Computing*, *supra* note 10, at 25.

52. *See, e.g.*, *AWS Customer Agreement*, AMAZON WEB SERVICES (March 15, 2012), http://aws.amazon.com/agreement (section 3.2) ("We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities."). *See also* Hon et al., *Data Export in Cloud Computing*, *supra* note 10, at 25-26.

53. Hon et al., *Data Export in Cloud Computing*, *supra* note 10, at 33 n.36.

54. However, an IP address may not always reflect geographical location. For example, a multinational corporate may route all communications through its United States headquarters, thus identifying them externally as having United States IP addresses, irrespective of local offices' locations.

ency regarding providers' systems, data center locations and transmissions.

Although the Data Protection Directive allows personal data transfers *within* the European Economic Area, many users, particularly public sector users, further require data centers to be within their own country. One provider stated that, because it did not currently use any data centers in the United Kingdom, it could not offer its solution to United Kingdom central government departments such as the Cabinet Office or Department for Works and Pensions, who required use of United Kingdom data centers only.[55] Integrators have also noted this position.

Our research ties in with the Cloud Industry Forum surveys, which found that seventy-five percent of United Kingdom users considered it important for data to be stored in the European Economic Area, with forty percent wanting data confined to the United Kingdom. Interestingly, while forty-one percent of users surveyed by Cloud Industry Forum wanted corporate data confined to the United Kingdom, the proportion increased for small and medium-sized enterprises as well as public sector users.[56]

Providers may attempt to address these issues by using partners with data centers in the required countries, or by using private clouds. While data location can be circumscribed by such commercial or technical means, this involves greater costs, because providers may not be able to use resources as efficiently.

Salesforce was cited as allowing users to check their data's location in near real-time with its trust.salesforce.com webpage. Possibly this is due to Salesforce's history of servicing business users, whereas many other cloud services' initial customer base is mainly comprised of individual consumers or small and medium-sized enterprises. Technically, providers may be able to engineer their systems to offer similar services. However, this will involve expense which may be passed on to customers, and, as mentioned above, verifying claimed data locations is still difficult technically.

Data location is a problematic, in some ways emotionally charged, issue. One global user said that if it could not ensure its data were confined to the European Union, it would nevertheless avoid the United States because of the United States PATRIOT Act and litigation issues. Financial institutions particularly raised this legislation. European Union providers and others have suggest-

---

55. This may seem little different from United States regulation, such as the International Traffic in Arms Regulatory framework, requiring that certain cloud services for federal government be housed in information technology infrastructure located in the United States accessible only to vetted United States citizens. For example, in 2011 Amazon launched a cloud service to comply with these requirements. *See* Werner Vogels, *Expanding the Cloud – The AWS GovCloud (US) Region,* ALL THINGS DISTRIBUTED (Aug. 16, 2011), http://www.allthingsdistributed.com/2011/08/aws_govcloud_region.html; *AWS Security and Compliance Center*, AMAZON WEB SERVICES, http://aws.amazon.com/security/ (last visited Dec. 12, 2012).

56. *CIF3*, *supra* note 13, at 8.

ed that data would be safer in, for example, a German-only cloud.[57] However, the United States is not the only nation that may access data for anti-terrorism or anti-crime purposes, and the current high profile of this Act may perhaps reflect some marketing opportunism, and certain political concerns regarding the United States exercising its powers extra-territorially, more than legal differences.[58] We discuss law enforcement access provisions further below.

Given the prevalence of remote access to data, data center location is not the only factor affecting data location. Many sources pointed out that a European Economic Area provider, with data centers confined to the European Economic Area, may, in order to provide round-the-clock "follow the sun" services, use support staff or sub-contractors outside the European Economic Area who have (or are given) access to customer data or metadata. Remote access to user data by affiliates or support staff or sub-contractors may involve "transfer." Even where such personnel cannot login to user accounts, they may be able to view metadata, such as when an e-mail was delivered. To troubleshoot account issues, sometimes users may give login details, including passwords, to support staff, in which case user consent may be assumed. However, where non-European Economic Area support staff have remote access to personal data (even when not given login details by individuals seeking assistance), and users have not been informed, it is not certain that users must be assumed to have consented to the transfer. One user called potential access by support staff "a huge hole," citing a provider who insisted its service involved no international data transfers because its data center was located in the European Union, seemingly overlooking the relevance of the fact that its support, maintenance and even code debugging might occur in India and that therefore personal data could be transferred to staff located in India. Some providers deal with this by using a recognized method of transfer to non-European Economic Area support staff or support sub-contractors, such as establishing contracts based on model clause terms.

Irrespective of data protection, existing contracts may restrict data location. For example, one global user's service, provided to end users over the cloud, includes provision to end users of licensed content subject to intellectual property rights. Certain content licenses required this global user to store the content on its own secured servers, and to know its location at all times. Obviously, such content cannot be stored in the cloud in circumstances where it could be distributed or moved across different data centers. Even within one data center, a user's stored data may migrate between locations, depending on systems

57. Cornelius Rahn, *Deutsche Telekom Wants "German Cloud" to Shield Data From US,* BLOOMBERG (Sept. 13, 2011), http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html.

58. Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent,* QUEEN MARY SCH. L. LEGAL STUD. RES. PAPER 74, 2 (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067.

used. Thus, some intellectual property rights licensing schemes may hold back cloud adoption, and licensors may need to be made more aware of how cloud storage works.

Other regulatory issues may be relevant. For example, export control laws were mentioned as restricting transfer of certain information or software to particular countries indicating that locations of providers and data centers may arise in that context as well, with remote access being, again, a thorny issue.

2. *Data processor agreements, and sub-processors*

Users who are "controllers" of "personal data" under the Data Protection Directive must comply with certain requirements when engaging "processors" to process personal data for them. The Data Protection Directive's minimum requirements have been increased by some states, so rules are not uniform across the European Economic Area.[59]

Many providers' standard terms are silent on the point, or at most state that the provider acts only as "data processor." This seems mainly for providers' protection, to try to ensure they are not regarded as "controllers" (with greater obligations and liabilities) even though contractual labels are not determinative.[60]

The Data Protection Directive requires the controller or user's contract with the processor or provider to contain an agreement, often referred to as a "data processor agreement", which states that the processor must process personal data only according to the controller's instructions and must take certain security measures. Some enterprise-oriented providers' standard terms may, to assist users to comply with the Data Protection Directive, specifically include a data processor agreement. Otherwise, users who are controllers of personal data may want it included. This is common, for example, in financial institutions' standard contracts.

However, some providers would not go further than stating their processor status. The underlying reason may be that the Data Protection Directive does not cater well to cloud processing. In particular, even treating infrastructure providers as processors may be inappropriate, as they provide users with information technology resources and suitable (but standardized) environments within which users may use those resources rather than actively processing data for users.[61] Providers have therefore considered it inappropriate to agree contractually to process data only on users' instructions as it is for users to control their own processing. With shared common multi-tenant infrastructure involv-

---

59. *See* Hon et al., *Who is Responsible for 'Personal Data' in Cloud Computing*, *supra* note 10, at 4.

60. *Id*. at 7-9.

61. *Id.* at 9-14 (analyzing these issues in detail).

ing one standardized environment for all users, it would be difficult, if not impossible, to comply should different customers issue different instructions regarding the environment or resources.[62]

That said, some providers have accepted a data processor agreement. Conversely, where providers would not agree anything more specific than general obligations to comply with data protection laws, one global user stated that it had accepted that with large providers who, from previous dealings, the user knew had implemented proper data protection processes.

Providers' terms generally entitle them to use sub-contractors, for example, to provide support services. One fundamental issue is whether cloud sub-providers are sub-processors of personal data. This Article assumes they are sub-contractors and sub-processors, although the matter is arguable.[63] Use of cloud "sub-processors" has arisen in several European Union data protection authorities' decisions or guidance; they consider that compliance requires controllers to know all possible sub-processors, perhaps even down to the data-center operator level.

Whether or not personal data were involved, some users wished to restrict sub-contracting (including of support services), and to provide contractually that providers' contractual obligations were unaffected by any sub-contracting. Users in large deals normally prohibited sub-contracting without their consent, except to providers on a pre-approved list and on certain mandatory terms. They sometimes asked to see the sub-contract, or even contracted directly with sub-contractors for obligations including confidentiality. One global user stated that, as with managed services, if any sub-contractors had access to data stored or otherwise processed by the user in the cloud (whether personal data or otherwise), or if any sub-contractors provided services worth more than a certain percentage of the contract value, it required rights to vet and veto them. For smaller deals the user wanted notification of any such sub-contractors' identities, but not necessarily veto rights. With SaaS, the user still inquired specifically as to sub-providers and their geographical locations. Similarly, other global users indicated they would not allow sub-contracting or assignments without express prior consent. One SaaS provider confirmed that some users insisted on consent as a pre-condition for assignments. Therefore, it seems that at least some users who have been able to negotiate contracts have required similar safeguards and pre-contract information, as European Union data protection authorities have required.

In summary, current data protection law puts both users and providers in a

---

62. A possible exception involves private clouds outsourced to integrators, where integrators may be able to comply with instructions regarding infrastructure dedicated to and customized for the user concerned.

63. *See* Hon et al., *Who is Responsible for 'Personal Data' in Cloud Computing*, *supra* note 10, at 6.

difficult position, with one or the other being required to take a view on the contract terms, accepting that a data processor agreement is necessary by law where personal data are involved, but noting that it may be meaningless or impossible to comply with a data processor agreement in the cloud. Investigation of any sub-providers, and possibly even data centers ultimately, may also be necessary for compliance.

3. *Data subject rights*

If data subjects request access to their personal data from users, one SaaS provider pointed out that, because users have direct access to and control over data (including any personal data) they choose to process using cloud computing, it should be unnecessary to involve providers. Users can retrieve the requested personal data directly themselves. Nevertheless, one global user secured from its global provider an obligation to co-operate with the user as necessary to respond to subject access requests, and similar wording is standard in United Kingdom government contracts, including the G-Cloud v1 framework agreement.[64]

Again, these sorts of contractual provisions, while they made sense for processing agents who have sole control of outsourced data, do not recognize the "self-service," tools-based nature of cloud computing.

D. *Confidentiality, and Rights to Monitor, Access, Disclose or Use Customer Data*

1. *Confidentiality*

Providers may receive or have access to two main kinds of confidential data: data disclosed by users during contract negotiations (such as information on intended purpose and usage of the service), and data processed via the service. In both cases, these may include personal or commercially sensitive data, in the latter case, possibly even customer or other third party personal data. Users may accordingly want confidentiality or non-disclosure agreements from providers. In some cases, users have secured unlimited liability for the former, but liability for the latter has proved more difficult to allocate, and can be a "show stopper."

Many users have persuaded providers to accept liability, usually capped, for breach of confidentiality, and generally users pushed for higher caps here. Users preferred capped liability from integrators to no liability or restricted liability under providers' standard terms. It was rare, but not unknown, for pro-

64. Hon et al., *supra* note 30, at 22 n.159.

viders to accept uncapped liability for breach of confidentiality, data disclosure, or data protection breaches, at least where limited to direct losses and excluding contingent liabilities or consequential damage. Enterprise-oriented providers seemed more flexible with highly regulated users, for example even giving indemnities for breach of data protection obligations. In contrast, one non-European Union provider stated it would never agree to any liability for breach of confidentiality.

Definitions of breach of confidentiality and the amount of the cap obviously involved careful consideration, for both users and providers, as did definitions of direct, indirect, and consequential losses. Some providers also considered that data loss should not be treated as breach of confidentiality per se, particularly with SaaS, capping such liability accordingly.[65]

Users negotiated for confidentiality obligations to survive termination of the agreement, typically for 5 to 7 years, depending on the data's nature. Some users even wanted such obligations to continue indefinitely.

2. *Access to user data; disclosure*

Users fear possible unauthorized access to their data. Many providers have "back doors" to access users' data, and contractually reserve access rights,[66] which they consider are needed for maintenance, servicing, support, or even security purposes. Their users may have to accept that support and perhaps other staff may access their data. Other providers stated they had no such access, although they could terminate users' access.

Even some providers who stated that they cannot access user data without customer login details reserved rights to access data for maintenance and the like, and acknowledged that certain employees could do so in "emergency" situations. In addition, users may volunteer login details to support staff when seeking assistance, although the extent of resulting access depends on that individual user's own access rights.

Regarding service usage monitoring, some users had not negotiated the issue, but others stipulated expressly that information obtained from such monitoring, or from support or maintenance activities, must be treated as confidential information subject to confidentiality provisions. Some users restricted contractually the purposes for which the provider could monitor use: for example, only for security purposes (such as filtering e-mail for spam or malware),

---

65. On "personal data" in cloud computing, *see* W. Kuan Hon, Christopher Millard & Ian Walden, *The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated?—The Cloud of Unknowing*, 1(4) INT'L DATA PRIVACY LAW 211 (2011). On responsibility for personal data in cloud computing, *see* Hon et al., *Who is Responsible for 'Personal Data' in Cloud Computing*, *supra* note 10.

66. Bradshaw et al., *supra* note 2.

or to establish and substantiate charges payable, such as how many end users had used a particular service, or to verify compliance with terms, for example size, capacity and bandwidth limits. Some users wanted to prohibit use of resulting data for any other purpose, and indeed prohibit monitoring for any other purposes. However, some providers would not agree to any restriction on their monitoring rights. Others stated they could not technically monitor processing performed by users, e.g., within users' VMs.

Standard terms usually authorize providers to disclose users' data on court order—or even if simply *requested* by law enforcement authorities.[67] Some providers would contractually agree to notify a user immediately upon law enforcement or other official authorities' requests for that user's data. However, certain laws may forbid such notification. Thus, the term would be qualified accordingly. Absent such standard terms, users have required providers to notify them promptly on receipt of any third party requests (unless prohibited by law), passing requests to the user (which integrators would send on to end users or customers), and allowing the user to make representations to resist disclosure. Indeed, financial institutions' standard terms may even prohibit disclosure altogether except with their consent, although they would accept that disclosures may be required under laws or court orders preventing providers from notifying users. In some cases, providers considered that users subject to specific lawful intercept requirements, notably telecommunications users, endeavored to pass off those obligations to providers.

One SaaS provider had users with specific requirements as to data location and ability to access data (e.g., never outside country X, must be duplicated in country Y as well as elsewhere, never in country Z, and so forth). It addressed those requirements by using affiliates and partners operating data centers in different countries. If an entity in one country was required by that country's laws to access data held in a data center in another country, it could not do so, because it had no control over that data—the affiliate or partner did.

E. *Security Requirements, Audit Rights, Security Breaches or Incidents and Incident Response*

Security is often cited as an issue in cloud computing—partly because of general concerns arising from loss of user control, and partly because data protection laws require controllers to take appropriate security measures to protect personal data. It may also be easier for users to obtain board approval for contracts specifying detailed security requirements and audit rights, demonstrating

67. Bradshaw et al., *supra* note 2; Walden, *supra* note 58. Nevertheless, 54% of United Kingdom users believed providers would give data to third parties only if required by court order, while 93% of United Kingdom users expected providers to contact them before releasing data. *CIF3*, *supra* note 13.

that a considered, structured decision had been taken on the security risks.

Accordingly, security often arose in pre-contract discussions, particularly as many providers were not forthcoming regarding their security arrangements. One global user noted, "It is a challenge to find out what protection providers are providing." Worryingly, a report in early 2011 on the security of cloud providers found that most providers, including large ones, did not prioritize security.[68]

Several sources cited problems with audit rights, particularly for financial services users, who require extensive audit rights for themselves, their financial auditors, and regulators.[69] Deals have fallen through because providers would not compromise on audit rights. One integrator commented that its users did not appreciate the level of resistance from providers on audit rights. Audit rights and certifications have been in issue with shared services generally, not just cloud computing.

Education is important, as it appears some users still lack sufficient knowledge about cloud components and services. For example, an integrator was asked to agree to audit rights where it only provided application software running on the user's own infrastructure.

1. *Providers' security measures: pre-contractual audits*

What security measures should be taken, and who is best placed to take them, will vary with the nature and type of service. With IaaS and PaaS, providers consider users have much more control over security measures, while SaaS providers generally have more control.

Regarding pre-contractual audits, for data protection and other reasons users wanted to know what physical and digital security measures providers took, to ensure providers had adequate security policies and underpinning systems, and that any issues were followed up in practice, with appropriate approval processes for configuration and change management. Users' security questionnaires might include hundreds of detailed questions, such as fire extinguisher locations.

However, providers generally considered that, particularly with shared in-

---

68. PONEMON INST, SECURITY OF CLOUD COMPUTING PROVIDERS STUDY (2011) (reporting a survey of 103 cloud service providers in the United States and twenty-four in six European countries). In contrast, a more recent survey of 300 senior European technology leaders, including executives, investors, policy makers and officials aligned with the technology market, found that, of respondents who ranked cloud computing as a top three area of potential growth, security (protection and centralization of data) was one of the features stated to most drive their company's adoption of cloud computing (at 58%). DLA PIPER INT'L LLP, THE EUROPEAN TECHNOLOGY INDEX (2012).

69. *See, e.g.,* FINANCIAL SERVICES AUTHORITY, SENIOR MANAGEMENT ARRANGEMENTS, SYSTEMS AND CONTROLS, 2009, 8.1.8 (U.K.).

frastructure and multi-tenancy, it would be detrimental to security and against their own security policies to provide full details of their security policies and practices to all prospective customers, or allow data center visits. In other words, too much transparency about security can itself compromise security.

One global user asks all potential providers for their security standards, which its security team reviews, and said, "Where we know we will be struggling with the provider because of their security standards, and they're not prepared to negotiate or change them, we'll go elsewhere." Some providers provided documentation or other information showing they take security measures. Generally, providers would at most allow users (or users' security teams) to see a summary or high-level overview of security policies, measures, and standards. Only rarely would a provider provide more detailed information than it made generally available. However, for the right deal or customer, typically government or financial services, one enterprise-oriented provider had, subject to non-disclosure agreements, allowed prospective users' security-vetted personnel to make escorted data center visits, view specific documentation such as its ISO27001[70] policies and procedures and other detailed information given to its certifier to support its certification, and discuss issues with teams providing or supporting services and application security, security monitoring, and so forth. However, they were restricted to viewing hard copies in closed rooms, with no ability to take copies.

One global user commented that Salesforce emphasizes its willingness to allow users to visit its data centers, whereas some others are less receptive to audits of their physical or logical storage and systems. For small deals, understandably providers may not be willing to allow numerous prospective customers to visit data centers and the like, although one SaaS provider, who disallows "pen testing,"[71] would allow "physical walk rounds" of sites, and another global provider also permitted site visits. This may depend on how much control the provider has. If it controls all relevant data centers, escorted "tours" are obviously less problematic, although they still involve resources and costs for providers (and, accordingly, increased costs for users). Some queried the value of physical visits, and indeed the Swedish data protection authority questioned their appropriateness with shared infrastructure, "since data from several players are stored in the same premises and access opportunities for all who store the data would result in security risks in itself."[72]

Sometimes, having information about the provider's security measures is

---

70. ISO27001 is an industry standard security framework for implementing information security management systems within an organization.

71. *See infra* Part IV.E.4 (for definition).

72. Datainspektionen, *Tillsyn enligt personuppgiftslagen (1998:204) – Salems kommunstyrelse* (2011), *available at* http://www.datainspektionen.se/Documents/beslut/2011-09-30-salems-kommun.pdf.

sufficient for users. One global user stated it did not necessarily negotiate detailed terms regarding security if, having seen the provider's documentation and been permitted access to its systems, it was satisfied with its security.

2. *Whose security policy?*

To what extent could users dictate security policies or practices? In a pre-cloud, single user scenario, such as traditional outsourcing to a managed services provider, a provider might well agree to follow the user's security policy.

However, where multiple users share standardized infrastructure, it would be difficult, if not impossible, for providers to comply with all users' separate security policies, with possibly different, even conflicting, requirements. Nevertheless, users often wanted to specify their own security policies (which they considered appropriate to the data's sensitivity), typically scheduled or annexed to the contract, with the provider undertaking to comply with those minimum measures.

Providers generally refused. At most, they undertook to comply with their own policy, perhaps specifically stated to be based on industry best practices such as ISO27001, usually reserving rights to change their own policy unilaterally—essentially on a "take it or leave it" basis. One global user noted that, having reviewed the provider's policy, for reasons of pragmatism it was willing to accept that position, at least for relatively low risk data. Even where providers' security policies already covered, for example, encrypting stored data, they might not necessarily make that a contractual commitment, although they might agree that, for example, only qualified and vetted employees who needed access to user data would have access.

Depending on the data's sensitivity, users may want more assurance on minimum-security levels than simply compliance with providers' own policies. For instance, some users wanted all data at rest and all connections to be encrypted.[73] Most users could not compel providers to undertake additional security measures, although some large ones, such as banks, could. One global user, after much negotiation, persuaded some providers to agree to follow the user's own security policies, although others refused. For another user, some providers agreed minor changes, but about half refused to meet higher standards. This may partly be due to reluctance to incur costs, sometimes significant, in obtaining and maintaining certifications such as ISO27001. A non-European telecommunications provider stated that, in one large deal, the user considered even ISO27001 inadequate, although there the provider was willing to receive the user's specific requests and consider implementation costs. Deal value seems highly relevant. For the right price and users, such as financial institu-

73. Whether providers have access to decryption keys is a different, important issue. *See* Hon et al., *Who is Responsible for 'Personal Data' in Cloud Computing*, *supra* note 10.

tions, some smaller providers were willing to accept higher security requirements—one SaaS provider even proved willing to agree to a financial institution's full standard security schedule.

According to our sources, many deals have fallen away, or "not even gotten to first base," because providers would not agree to follow users' security policies. One global provider felt that in such situations, the user was simply not ready to move to the cloud.

3. *Certifications*

Independent certifications to objective industry standards may be a possible compromise to address security issues. Industry standards and certifications specific to cloud security have not been fully developed, although organizations like the Cloud Security Alliance, Open Data Centre Alliance and Cloud Industry forum are progressing matters. Whatever standards are adopted need to be cloud-appropriate. One provider commented that some customers, especially governments (United States, European Union including United Kingdom) or government contractors, required Evaluation Assurance Level certification under Common Criteria security evaluation standards.[74] However, those specify particular hardware or software rigidly, with certifications being invalidated on changing the relevant hardware or software, —so they do not suit the cloud, where hardware used may be unknown, and products evolve quickly. That provider said, "It is complex and expensive to get official certification for so little certainty."

One enterprise-oriented SaaS provider stated that all of its customers raised security as an issue, but after conducting their due diligence and noting the service's certifications such as for credit cards (PCI/DSS),[75] ISO27001, and SAS70[76] certifications, they were more reassured; indeed, some were satisfied that the security level far exceeded their internal security protections. Some providers undertook to obtain and maintain industry standard certifications such as ISO27001, providing users with copy certifications and so on. One global provider undergoes regular SAS70 type II audits by an independent au-

---

74. COMMON CRITERIA, COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION (2012).

75. PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD (2010). Note that a provider's PCI/DSS compliance does not automatically mean its users are compliant, as that requires further action "above the hypervisor," within the purview and control of users rather than the provider. Marcia Savage, *PCI DSS Compliant Cloud Providers: No PCI Panacea,* SEARCH CLOUD SECURITY (Mar. 22, 2011), http://searchcloudsecurity.techtarget.com/news/2240033583/PCI-DSS-compliant-cloud-providers-No-PCI-panacea.

76. AM. INST. OF CERTIFIED PUB. ACCOUNTANTS, STATEMENT ON AUDITING STANDARDS NO. 70 (1992). Replaced in June 2011 by AM. INST. OF CERTIFIED PUB. ACCOUNTANTS, STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS NO. 16 (2011).

ditor, sharing reports with users.

Other certifications or security assurances may be considered regarding software infrastructure, such as on the effectiveness of virtualization platforms for segregating users. In September 2011 the CESG (United Kingdom National Technical Authority for Information Assurance) assured VMWare's VSphere 4.0 hypervisor for hosting, on the same platform, VMs for United Kingdom public sector information, protectively marked Restricted (Business Impact Level 3 or IL3[77]) and below.[78]

4. *Pre-contractual penetration testing*

Pre-contractual due diligence measures for users may include security penetration testing ("pen testing"), to check security issues such as integrity and robustness of providers' security policy and information technology systems, and how (and how well) users' data or instances are separated from other users' data.

Many users, particularly from regulated sectors, wished to conduct pre-contractual pen testing. However, most providers would not agree, because of potential adverse impact on other users' services or data. An enterprise-oriented public SaaS provider confirmed it often received such requests from large organizations, particularly financial institutions. That provider had occasionally agreed, subject to the user's agreement to accept unlimited liability for any damage caused and to constrain testing as regards timing, from which IP address, and so on. Any agreed pen testing would usually be confined to a sandbox, a special segregated area, to avoid possible damage to systems that could affect other users. Numerous pen tests were conducted on this basis annually. Some automated scanning of the application was permitted, at weekends only. However, that provider still did not permit unlimited pen testing.

Providers that disallow user pen testing may conduct their own tests (or use a third party), sharing results with current or prospective users. One SaaS provider organizes its own regular third party pen tests, including after application upgrades, and shares summarized results with users. Some users required sight of such results before contracting. Others still wanted their own or third party pen tests. Another SaaS provider stated that it was obtaining SAS70 certification[79] to address users' desire to conduct their own pen testing.

---

77. *See* CESG & CABINET OFFICE, EXTRACT FROM HMG IA STANDARD NO.1 BUSINESS IMPACT LEVEL TABLES (2009).

78. CESG, *CAPS Product Results*, http://www.cesg.gov.uk/finda/Pages/CAPSProduct.aspx?PID=176 (last visited Nov. 15, 2012). *See also* CESG, CESG AND VMWARE DELIVER TRUSTED PLATFORM FOR HOSTING MULTI-LEVEL ENVIRONMENTS (Sept. 14, 2011), *available at* http://www.cesg.gov.uk/Publications/Documents/cesg-vmware_joint-statement14-09-11.pdf.

79. Replaced by SSAE 16 from June 2011. *See* AM. INST. OF CERTIFIED PUB.

Ongoing user pen tests were unusual. One global user, after conducting pre-contractual pen testing on a global provider, without a physical site audit, was satisfied by that test together with undertakings to comply with security measures, without requiring rights to conduct future pen tests.

As a non-European telecommunications provider pointed out, it would be impossible to stop users from pen testing if they wished to conduct them. Interestingly, although that provider had several large users including banks, it commented that none sought prior security testing, although all requested security certifications.

5. *Ongoing audit rights*[80]

Regarding post-contract audits, many financial services users felt they needed providers to commit to allowing audits at least when the user's regulator (or its end user's regulator) required it. However, most providers refused for reasons of security and costs, although providers were more willing to allow audits if users met all costs. Even enterprise-oriented SaaS providers that allowed audits would not offer the unfettered audit rights required by financial institutions. They generally restricted them narrowly, for example once a year per user, only if the user's regulator required the audit, or only with their prior consent. Or, they might agree to provide only "commercially reasonable" cooperation rather than full audit rights.

Several European Union data protection authorities consider that users need technical and practical means to investigate suspected unauthorized accesses to personal data, whether within the user or provider, meaning contractual rights to logs or audits. Some providers offer users tools to monitor accesses to user data, not just logs but also real-time 24-hour monitoring, so users may check who has accessed which accounts, what they viewed, and what they did. One SaaS provider stated that it undertakes to log all accesses as standard. It commented that, once this undertaking was pointed out, most users who requested audit rights were content to rely on access logs instead. Provision of such tools by more providers may help increase user trust by increasing transparency, as well as assisting with legal compliance. Some authorities also consider that, apart from access logs, for users to check providers' compliance with required security measures, ongoing post-contract audit rights against all sub-providers would also be needed—IaaS, PaaS, perhaps even down to the data

---

ACCOUNTANTS, *supra* note 76.

80. For a detailed survey and guide to ongoing security service level agreements, *see* European Network and Info. Sec. Agency*, Survey and Analysis of Security Parameters in Cloud SLAs Across the European Public Sector* (2011); European Network and Info. Sec. Agency, *Procure Secure: A Guide to Monitoring of Security Service Levels in Cloud Contracts* (2012).

center level.[81] Clarity is needed regarding how far down the "stack" users must go.

A global integrator commented that providers' reluctance to allow audits might partly arise from their not necessarily being able to pinpoint exact locations of users' data.[82] Also, providers may not have sufficient control or rights to allow audits, especially if using sub-providers. In concrete terms, consider a SaaS provider using a PaaS provider's service, which may itself use a third party's IaaS infrastructure or data centers. The SaaS provider may, if it chooses, permit inspection of its application code to verify application security – but it may not be entitled to permit users to audit the PaaS or IaaS provider or visit data centers, or even conduct its own audits of sub-providers. Therefore, rights to audit sub-providers may be problematic. That said, one financial institution was able to require comprehensive audit rights from a United States SaaS provider for itself, affiliates and regulators, including sub-providers and subcontractors.

One compromise in which integrators were involved was for providers to agree to share their own audit reports with the integrator, or at least allow the integrator to view the reports, and ideally (though many providers might not agree) allow it to share the results with its own users and their regulators. Where audits are disallowed and no independent third party audits are conducted or shared with users, users must rely on providers' undertakings regarding security (if any). Compliance verification there would be impossible. A global user noted, "The only way to find out if they have actually complied is if they have a major breach or loss of confidential information!"

The general lack of audit rights causes difficulties, especially for integrators whose customers require audit rights, possibly even including rights to select auditors. This issue may loom larger in future as audit rights increasingly come to the fore—described by one user as a "headache," with users being dependent on the (not necessarily consistent) views and actions of individual national regulators. Ongoing third party audits to industry standards could be considered as a possible solution, as with pre-contractual audits, but legislators and regulators need to consider these issues, particularly the extent to which users may rely on such audits for liability purposes.[83]

---

81. Datainspektionen, *supra* note 72. This view was also taken in mid-2012 by European Union data protection regulators collectively. *See* Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, Working Paper 196 (Jul. 1, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

82. *See* Hon et al., *Data Export in Cloud Computing*, *supra* note 10, at n.36.

83. For example, some data protection authorities (for instance, Sweden's, *see* Datainspektionen, *supra* note 72, at 16) consider that independent third party audits would not absolve controllers from responsibility to ensure appropriate security measures were in fact taken.

6. *Security breach notification*

Many providers' standard terms did not require security incidents to be reported to users. This may have been for operational reasons as many providers' systems and processes were not originally set up to enable them to notify users of incidents easily and quickly.

Users have requested notification of data losses or security breaches at, the provider level in, say, twenty-four hours, sometimes even when only other users were affected. Some providers agreed to notify users promptly of breaches or losses, at least where affecting that user (but possibly not if only affecting other users). Others, while not committing contractually to notify users, would in practice attempt to notify users as soon as possible, although in some cases faster notification was possible if the user paid for higher support levels. Still other providers would not commit to notifying users, except perhaps for specialized users such as telecommunications providers who by law need that capability, but are putting into place systems and organizational measures to enable them to do so in future.

For large users, some providers have been willing, if the matter goes to a senior enough level, to accept additional obligations to use commercially reasonable efforts to monitor for and detect breaches, and to notify of breaches (at least where affecting that user), perhaps also with rights for the user to terminate for the breach. The notification period may be short, for example within one business day after the provider becomes aware of an actual or potential threat, at least where it may adversely impact on the user's service, such as unauthorized access. As with other important notices, users may require notification to be in writing to a particular address, not just by e-mail.

As regards actions providers must take after security breaches, the agreed security standards usually addressed the position, for example by requiring isolation or quarantine of affected areas, and otherwise remedying the situation.

On receiving notification, some users wanted their security team to investigate and consider whether the provider had met the required security standards, and if they had not, the user wanted rights to serve notice to remedy the breach, if not already remedied, or even to terminate the agreement. Unlike with traditional outsourcing, however, many providers would not agree to any joint analysis of the breach with users, but insisted on dealing with breaches themselves.

F. *Lock-In and Exit*

Many users cited lock-in as one of their top concerns with the cloud. There are several aspects to lock-in. Exit strategy and end-of-contract transition were major concerns amongst users, including data portability, and the importance of retaining metadata as well as data. Users may not wish to be "locked in" or tied down for too long an initial contract term—this seems essentially a commercial issue, often linked to pricing, sometimes negotiable. We cover this later.

A major lock-in concern is risk of dependence (or over-dependence) on one provider's, often proprietary, service. If the service is terminated for whatever reason, users wanted to recover all their data and metadata in formats that are easily accessible, readable, and importable into other applications, whether running internally or in another provider's cloud. This is commonly called "data portability." Application portability is one aspect of dependence risk which is not discussed as much as data portability, whether by our sources or in the literature. However, it is equally if not more important, particularly for IaaS and PaaS. As cloud use becomes more widespread and sophisticated, we believe future contract terms may extend to cover application portability, virtual machine portability, and perhaps even interoperability.

1. *Data retention, deletion and data portability*

Two issues arise with data retention and deletion. The first is, will providers retain users' data when needed by users, so users can retrieve data in usable format? The second is, will providers delete user data when required?

There are two main circumstances when users may wish providers to retain data: where data needs to be retained for purposes of regulation, litigation or other legal reasons affecting users; and after contract termination, where users want providers to retain users' data for a long enough period after termination to allow users to recover their data.

Data retention for legally required purposes, such as litigation e-discovery or preservation as evidence upon law enforcement request, has not been negotiated much yet, according to our research. A large enterprise-oriented SaaS provider stated no prospective user had raised the issue until early 2011. We think it will become more important in future. One aspect is how much, if any, assistance providers give users. For example, an enterprise-oriented provider stated, if users needed to retain data for longer periods, such as for tax reasons, they had to arrange their own storage. A global user was concerned about using a particular large provider because it did not know what, if any, processes that provider had implemented for e-discovery, whereas another platform it used did have such processes. Another global user stated it had secured a global provider's agreement to retain, segregate and secure data if specifically requested, while a SaaS provider specializing in e-mail continuity provides, as standard, tools to assist with e-discovery, offering users a choice of retention periods, longer periods costing more.

These examples illustrate that data retention for compliance is technically possible. However, e-discovery tools for the cloud still seem to be lacking. One user commented that providers often had difficulty understanding that the user would need their help should it receive a relevant request. Users have defined contractually exactly what assistance they may need from providers here.

Users' ability to have data returned upon contract termination has seen more negotiation. Process simplicity may be as important as data format. A

United Kingdom public sector educational institution chose one provider's SaaS service over another's partly because it believed it was easier to retrieve data from the former.

There are several aspects here: data format, what assistance (if any) providers will give users, what if anything providers charge for such assistance, and data retention period.

Some providers, especially enterprise-oriented ones, commit routinely to return users' data in standard format (typically CSV) on termination, at least upon the user so requesting. Several users mentioned they use Salesforce SaaS, one benefit being the return of data in common CSV format, as well as, with certain services, the possibility of weekly downloads or e-mails of their data. Some global users requested contractual commitments regarding return of data in their required format after termination for whatever reason, which some providers agreed (at least for reasonable formats), although sometimes this would be at additional cost if substantial quantities of data were involved.

Most providers did not offer any assistance, even contracted paid assistance packages. However, a SaaS provider stated that it assists in providing data in a different format for a set fee if requested by the user, while a global user noted that some providers or integrators would agree to provide assisted migration at contract end. A non-European telecommunications provider stated that it assists with migration in ("onboarding"), and, while willing to assist with migration out, found even its smaller users did not need it, as they took their own direct copies.[84]

Another lock-in issue is how long after termination users have to recover data before deletion. Many providers delete all data immediately or after a short period (often thirty days), but some users obtained longer grace periods, for example two months, perhaps requiring notice to users before deletion. Some providers offered longer periods, such as ninety days. For large deals, parties could agree on eighteen months to two years, with assistance for migration, more like classic outsourcing deals—although six months might suffice if providers agreed to provide "reasonable assistance." The period needed to migrate user applications and data would of course depend on the circumstances.[85]

Regarding deletion, standard terms may require providers to delete data after termination only if the user so requests, or are silent on deletion. However, depending on the type of service and intended usage,[86] users have sought con-

---

84. Cloud Industry Forum recommends that providers should assist with migration or at least allow users sufficient time to self-migrate. *CIF3*, *supra* note 13, at 15.

85. This paragraph was derived from our interviews. Additionally, Cloud Industry Forum recommends that providers should give at least thirty days' notice before deletion. *Id.*

86. Data deletion is often an issue in the cloud, but may be considered unimportant for some services. For example, for a SaaS service involving temporary processing but no permanent storage of data, a global user was not concerned about data deletion provisions even though personal data might be involved.

tractual commitments to ensure deletion of data from the provider's systems (including any duplicates or backups). This is relevant both when users delete data while using a cloud service, and after contract termination. Deletion after termination may be particularly important with personal data, including data held by any sub-processors.

As with local computers, when "deleting" cloud data, often data are not actually deleted. Instead, "pointers" recording locations of different data fragments, are deleted, and data are overwritten by fresh data over time.[87] Deleting data, rather than pointers, is more complex, and for better security requires overwriting a minimum number of times, the ultimate measure being secure destruction of physical storage media. Deleting data from backup tapes is even more difficult. Also, if cloud data move between different equipment automatically, data may remain in previous devices until overwritten.[88]

One SaaS provider splits data into smaller portions randomly after termination of the user's account, so it would be virtually impossible for users (although not the provider) to reconstruct data. It had received requests to commit to stronger deletion, but would not agree, although it would certify it no longer held data after their return. A global provider would agree to delete all duplicates (although it was unclear to what standard[89]), and also to certify deletions.

There are different locations and media from which data may require deletion, and different levels of deletion, up to destroying physical hardware securely. The degree of deletion required depends on the level of security required for the data concerned.

More secure data deletion is more expensive for providers (particularly destroying rather than redeploying equipment). Accordingly, they did not employ more secure methods unless necessary, and would want to pass on costs to users. Deletion seems as much a financial as technical issue. Costs may be partly why, as a global user noted, data deletion has not hitherto been a particular focus of cloud. A global integrator commented that providers would offer to delete data, but were reluctant to do so to ISO standards as they wished to reuse hardware. Where secure deletion was vital, as with financial institutions or telecommunications providers, some providers were willing to guarantee it—but usually only at greater cost.

Some global users had successfully required providers to delete data if requested, providing evidence of permanent deletion of all copies. Some users

---

87. Google notes this in its standard terms for Google Apps. *Google Apps for Business (Online) Agreement*, http://www.google.com/apps/intl/en/terms/premier_terms_ie.html (accessed Nov. 15, 2012), at section 10.4.

88. This issue was not generally covered in contracts, although it is noted by, for example, German data protection authorities' cloud guidance, *see* DATENSCHUTZBEAUFTRAGTEN, *supra* note 18.

89. For an example deletion standard, *see* CODE OF PRACTICE, Secure destruction of confidential material, BS EN 15713 (British Standards Inst. 2009).

would not contract with providers who did not so agree. A non-European telecommunications provider agreed to contractual terms requiring deletion, including specific provisions for overwriting data to recognized data deletion standards to make data unrecoverable, if larger users so requested. One global user secured additional obligations to deliver all backups of stored data and applications within a short period after termination. However, the most another global user secured was acknowledgement of data confidentiality, and warranties that data would be deleted following termination.

During the term, some users wanted rights to ensure data they deleted were deleted permanently, including all duplicates, such as after receiving complaints about end user intellectual property rights breach, or law enforcement requests for deletion. To assure the third party regarding deletion of all offending content, one compromise was to agree that providers must use reasonable endeavors to delete data and erase relevant storage media, when specifically requested by the user. Providers might also need capabilities to quarantine rather than delete data, for example with intellectual property rights disputes.

There may be an educational issue: users and third parties may need more explanation regarding degrees of deletion, depending on nature and sensitivity of content. If certain data are no longer accessible for most purposes, that might suffice in some situations, whereas more sensitive data such as customer payment records might require absolute destruction, or at least more secure deletion (and more stringent or frequent audits). The same situation arises where third party contracts, like certain content licenses, restrict where users may store data or applications. One provider noted another educational issue: users may need to make employees aware that, for example with SaaS services, 'deletion' often merely transfers data to a "recycle bin," stored for say 90 or 180 days, before deletion.

G. *Term and Termination*

1. *Minimum term, renewals and notice periods*

Our sources felt that, before contracting, users needed to consider carefully the minimum and maximum term acceptable to them and their exit strategy, and ensure their practical requirements were addressed contractually if necessary. A long initial term may be one aspect of lock-in.

One global user felt there was some "cloud washing," in that certain services described as "cloud" did not in fact utilize typical cloud pricing models or cloud technologies, for example because those services required minimum revenue and term commitments (unlike the "pay as you go" model meant to typify cloud), new servers had to be procured if more capacity was needed (instead of instantly increasing capacity on demand). However, even with acknowledged cloud services like Salesforce, a minimum term was often said to be required. A global user pointed out that larger users were better able to "beat cloud pro-

viders down on price," and therefore deals might be less commercially viable for providers unless longer-term. Bigger deals, or deals involving more sophisticated or customized services, were more likely to involve an initial minimum term, and there are indications that initial fixed terms are increasingly common. The question of initial minimum term is more a commercial than a legal issue, with some providers being willing to reduce unit or per-user prices for longer initial terms. Some providers wanted early termination fees (which may be "huge") if users terminated a fixed-term contract earlier for convenience, as recovery of fixed set-up costs were designed to be spread over the term.

Providers preferred fixed-term, at least initially, to rolling monthly contracts. Standard terms typically stipulate a one to three-year initial term, sometimes renewing automatically unless terminated. Cloud Industry Forum research[90] indicated forty-six percent of United Kingdom users' contracts renew automatically, particularly with smaller organizations, but only thirty-eight percent of integrators' contracts. The critical difference was that sixty-four percent of integrators' internal business practices incorporated early warning systems to manage renewals proactively.

As contracts often require notice of non-renewal within a set period before expiry, users could miss the window. Many users successfully requested deletion of automatic renewal provisions, or increases in the period before term expiry within which users could give notice, say from thirty days to sixty days. Because some users had apparently failed to understand the rollover mechanism, one SaaS provider even sends automated reminders at intervals in advance of that period. It seems users may need to improve contract terms or internal processes regarding renewals.

Length of initial term, and therefore period of lock-in, varied with type of service and deals. Some basic click-through SaaS services may be on a rolling basis, say monthly or ninety days. However, other SaaS services, particularly large deals, may have an initial fixed term and may involve master agreements. Terms sought by integrators depend on their customers' requirements. Some users, like financial institutions, might require even longer initial terms with guaranteed renewals, because they needed price ceilings over a longer period and required significant transition periods. However, providers generally did not offer initial periods as long as five years, so such users had to agree to shorter terms than they wished, and must devise advance plans for dealing with end-of-term issues.

Where terms permit termination for convenience by either party, notice period was another issue. To give enough time to migrate providers, users often needed longer notice from providers regarding service termination, than for notice merely of service changes, such as several months instead of one. This was particularly so with mission-critical applications, or with IaaS/PaaS where users

90. *CIF3*, *supra* note 13, at 6; *see also CIF2*, *supra* note 33, at 12.

might need to modify their hosted application's code to run on another provider's cloud. Accordingly, many users stated they always requested longer than the typical thirty days. Thus, portability and migration of applications, not just data, can be important for users. Ideally those aspects should be checked during due diligence (such as testing ability to export data to desired formats), rather than relying on the contract, as data and applications may require migration not only on contract termination but also should providers become insolvent or close down.

Conversely, some users wanted rights to terminate for convenience on shorter notice. For example, one global user negotiated longer notice from its provider than it had to give itself, although identical notice periods for both is not uncommon.

Users also risk lock-in in practice if, for example, their developers mainly use one provider's IaaS/PaaS service. While they can develop and leverage expertise in that service, they may also prefer to continue using it, given inevitable learning curves with other providers' services. Some users therefore encouraged employees to use several providers, to avoid over-reliance on one provider's service and its (possibly proprietary) application programming interfaces. If cloud services become standardized, the "internal expertise" issue may become less important. The use of proprietary versus open source cloud infrastructure will probably become a more significant issue in future.

2. *Termination events*

Insolvency and material breach are common events allowing termination. One global user did not want providers to terminate for anything except non-payment, as even an insolvent user may need continued use of cloud services while winding down business. A financial institution using its own standard terms stipulated non-payment as the only event entitling providers to terminate. However, generally providers seemed unwilling to remove other termination events, such as material breach and insolvency. One provider considered its termination events "set in stone" and would never agree to changes, unless perhaps the deal was large enough and the user would walk away without that change.

Regarding termination for non-payment, some users increased the notice period given by providers before such termination. For other types of breaches, integrators and other users who use cloud to service their own multiple end users had problems with providers' rights to terminate immediately on issues such as material breach, breach of acceptable use policies (AUPs) (covered below), or upon receiving third-party complaints regarding breach of their intellectual property rights. Such users did not wish actions of one end user custom-

er to trigger rights to terminate the whole service.[91]

However, many services lack granularity. For instance, an IaaS provider may not be able to locate and terminate the offending VM instance, and therefore need to terminate the entire service. Providers, while acknowledging this deficiency, still refused to change terms, but stated they would take a commercial approach to discussions should issues arise. Nevertheless, some users managed, though not without difficulty, to negotiate for notification from providers of any third party complaints regarding intellectual property rights infringement, no termination or suspension of service without further notification, and cooperation with the user as it tried to resolve the matter with the relevant end user or third party, perhaps by terminating just the offending end user's account with it. Users with multiple applications also sought to limit termination to a particular application, rather than all applications hosted with that provider.

Breach of providers' AUP may be a specific termination event, or material breach entitling providers to terminate.[92] AUPs tend to be "take it or leave it" and were not often negotiated, possibly because such terms were generally accepted as reasonably standardized, and providers considered them "hardcore." For instance, continually exceeding agreed usage limits would be considered unacceptable. Nevertheless, one global user negotiated successfully with a global provider for a less restrictive AUP, with fewer usages being stipulated as unacceptable.

For many users, AUPs were unimportant, although rights for providers to change AUPs unilaterally were not, as AUP breaches usually entitle providers to terminate. As mentioned, AUPs were problematic for integrators and others using cloud to serve their own end users, particularly consumers. One end user or customer breaching a provider's AUP may put the integrator or user in breach, enabling the provider to terminate services for the user and all other end users. Therefore, such users ensured that their end users were contractually obliged to comply with providers' AUPs, with end user accounts being terminable for breach. Instead of standard providers' terms enabling instant termination, they required providers to give notice before termination for breach of AUPs (except perhaps for material breaches), of say thirty days to enable users to remedy the breach, and obliging providers to consult before termination. One global integrator considered this a "huge" issue that did not get attention because of emphasis on liability and service levels. In its experience, most providers were willing to give some notice before termination, but not necessarily to afford users opportunities to remedy breaches, which it considered vital.

---

91. Forty-six percent of United Kingdom integrators had actively engaged with providers to define and determine termination events. CIF3, *supra* note 13, at 9. Perhaps smaller integrators had not yet focused on this issue, and/or few integrators polled were providers themselves.

92. Cloud Industry Forum research showed 70% of United Kingdom users had checked AUPs to ensure they were comfortable with them. *Id*.

Regarding users' termination rights, some users ("only the better lawyers," one SaaS provider noted) wanted termination rights for change in control of providers, for example if taken over by the user's competitor, with the usual issues regarding definitions and scope of "change of control," while users such as financial institutions wanted rights to terminate if required by regulators, law or regulation. Providers generally did not agree, except perhaps for large deals in specific circumstances with clear definitions of "competitor." While material breach is a common basis for termination, some users secured specific termination rights for defined breaches, such as breach of confidentiality, security policies or intellectual property rights provisions.

3. *Suspension*

Standard terms usually reserve rights to suspend services, such as for non-payment. This obviously affects users' services, and some requested changes, which were sometimes agreed. However some providers had no suspension rights, preferring simply to terminate for breach.

Like termination, suspension for breach of AUPs etc, was a particular issue for integrators or users with multiple end users, as services for all end users could be suspended for one end user's actions or omissions. Accordingly, one global user would not permit suspension except with prior notice and its agreement. An integrator would not allow suspension for any reason other than non-payment, unless prior notice was given, including reasons for suspension, so it could notify its end users and discuss it with them as appropriate. Another global user similarly required prior written notice of non-payment, with a final notice, before suspension was allowed, and a commitment to restore services within a certain number of days after payment. Other global users, including an integrator, agreed to allow suspension for breach, but again only after reasonable prior notice (which might be quite long in some cases), good faith consultation with the user, or other requirements. One financial institution did not permit suspension on any grounds, which the provider accepted.

Of course, suspension for reasons unrelated to users may be necessary, such as following a security incident, or to deal with technical service problems, so users generally have agreed to that kind of suspension.

H. *Changing Service Description or Features*

Many standard terms allow providers to change certain or all contract terms unilaterally.[93] This was seen by interviewed users as unacceptable. Again, enterprise-oriented providers were more likely to agree, or stipulate as standard, that amendment was only permitted if agreed in writing by users, or

93. Bradshaw et al., *supra* note 2, at § 5.2.

at least that users would receive prior notification whereupon they could terminate.[94] The latter was more common.

In particular, providers' right to change unilaterally service features, functions or even service description, was much negotiated. One non-European telecommunications provider stated that it notified its (enterprise) users of service feature changes, but would not necessarily contractually undertake to do so. A SaaS provider stated it never discontinues features, only introduces improvements, which customers could choose to enable. Its standard terms already stipulated that new features must not materially decrease users' functionality. The importance of this issue, and how much users negotiated it, varied with type and usage of service, extent of termination rights. For example, where users could terminate for convenience on giving notice, if a user disliked a feature change it might simply terminate.

With commoditized SaaS services, users might have to accept providers' rights to change features, although many users still wanted a qualification that changes must not adversely affect their service. For IaaS and PaaS, however, changes might be more significant, as they could result in users having to rewrite application code created to integrate with proprietary provider application programming interfaces, which users obviously wished to avoid. With large deals for mission-critical services, for example a global user's main platform for servicing its own end users, a provider's refusal to change this term could be a deal breaker. Therefore, users have insisted providers cannot change core services without consent, although minor changes to service features or support aspects might be permitted without notification. Service improvements were permitted. If changes were materially detrimental to their service, however, some users negotiated rights to terminate (or even to reject changes), at least upon the current contract period expiring, without liability but possibly without any rebates either.

Users generally also wanted longer prior notification of key changes and their impact, of at least thirty days or more. Certain providers who would not relinquish rights to change service features unilaterally still agreed to notify such changes, although not necessarily for longer periods or even in advance. Users wanted notice periods long enough to allow them to assess changes, discuss them with their own customers where relevant and, for changes considered detrimental, perhaps commence negotiations with new providers and give notice to terminate the contract. If providers guaranteed a longer lead time, say a year, before introducing notified changes, users were more comfortable with being able to adapt in time.

---

94. Cloud Industry Forum recommends providers should not be entitled to change terms without consent, or at least should give users notice and allow them to terminate. CIF3, *supra* note 13, at 14.

I. *Intellectual Property Rights*

Intellectual property rights issues frequently arise regarding cloud-processed data and, or, applications, including the cloud service itself. Indeed, for one global SaaS provider, they were negotiated the most.

Providers' terms may specify they own deliverables, for example documentation. Some users wanted clarification that users retained ownership of cloud-processed data, confidential information and so on. Some providers' standard terms do so provide.[95]

Standard terms may not address who owns rights to applications users develop or deploy on IaaS/PaaS. Some users wanted clarification that users own such intellectual property rights. However, the line is sometimes unclear between a user's application and the provider's platform and integration tools. In one deal, involving customization, a global user secured only an exclusive use period. Where integrators develop applications for their own customers, customers might require intellectual property rights ownership, or at least rights to use the software free after contract termination or transfer.

Another issue of contention concerned ownership rights to service improvements arising from user suggestions or bug fixes. Providers may require users to assign such rights. Yet users may not want their suggested improvements to be made available to competitors. Such users sought to prohibit provision of those improvements to providers' other customers, without the user's consent. This issue has arisen even in a deal involving open source software, where the user could not claim rights, let alone forbid using bug fixes for competitors.

Some cloud services include application licenses, and some users wanted clarification that pricing covered such licenses. However, other services do not include application licenses. To install user-sourced third party applications on IaaS/PaaS, or even some SaaS, users must "bring their own" licenses. Providers wanted express clarification of users' entitlement to load and use such applications on providers' infrastructure, even if the provider could not run them itself.

Only some application licensors allow users to "port" on-premise licenses to a cloud environment. Although not directly affecting contract terms, such licensing may be problematic for users. For example, logging usage in a VM may be unworkable, as they are continually instantiated or terminated, which may make it impossible to identify VM locations and which run licensed software. Rights to bring a set number of licenses to the cloud, irrespective of VM

95. Cloud Industry Forum research found nearly 75% of United Kingdom users (and 68% of integrators) were content that providers' contracts did not allow providers to take ownership of data/IPR. *CIF3*, *supra* note 13. *See* Chris Reed, *Information "Ownership" in the Cloud,* QUEEN MARY UNIVERSITY OF LONDON, SCHOOL OF LAW, Legal Studies Research Paper No. 45/2010 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.

location, would assist. One SaaS provider noted that, even when existing licenses could be "converted" to cloud, including the payment model, licensors' sales or marketing teams did not necessarily publicize that benefit, possibly because the commission structure was not so remunerative.

Licenses are charged on different bases, such as annually in advance for on-premise, and monthly rolling per user for "in-cloud." Some licensing schemes were preferred by SaaS providers for better matching provider-user payment models and being more suitable for public multi-tenanted cloud environments, such as Citrix's, which allows monthly per-user payments, as compared with, for example, Oracle's, which charges based on number of processor cores in the system used.[96]

CONCLUDING REMARKS

With initial adopters of cloud computing mostly being individual consumers or small and medium-sized enterprises, cloud computing epitomizes information technology's increasing consumerization as well as commoditization. The common use of providers' standard contract terms in cloud computing reflects the consumer distribution model. However, many factors are combining to force providers to become more flexible in their terms.

From the supply side, integrators, traditional information technology services vendors and telecommunications providers that are willing to accept more risk are increasingly entering the market, seeing the opportunity to sell more robust, enterprise-grade services, with contract terms to match—rather than the "as is, where is" services such as Amazon EC2 and Google Apps offer. Increasing availability of open source components such as OpenStack may also facilitate market entry by new providers, which may increase competition.

The market, while becoming more sophisticated and transparent than three years ago, seems to be fragmenting. There will still be bigger providers offering generalized "one size fits all" commodity services. However, niche providers and integrators are emerging, who are more willing to tailor services to user needs, whether contract terms or service features. Therefore, in order to remain competitive, providers may have to be more aware of user concerns, more flexible in negotiations, and more willing to demonstrate the security and robustness of their services.

Even large providers are realizing that, to gain or keep customers from cer-

---

96. *See, e.g.*, Bill Claybrook, *Warning: Not All Cloud Licensing Models Are User-Friendly*, SEARCHCLOUDCOMPUTING (Aug. 2011), http://searchcloudcomputing.techtarget.com/feature/Warning-Not-all-cloud-licensing-models-are-user-friendly. Oracle's charges equate each virtual core with a physical core (although one physical core could support several virtual cores) or vary with the number of virtual cores that Amazon EC2 instances used possess.

tain sectors, they must adapt accordingly. Several global providers are offering different services with different pricing and sets of terms, from consumer-orientated to enterprise-oriented, with specific terms for certain market sectors or functionality, such as third party-certified services.

Large users who were able to require that contracts be on their own standard terms are moving to make their terms more cloud-friendly, with some financial institutions beginning to consider producing standard SaaS and possibly even IaaS terms. Indeed, there may be scope for coordinated collective efforts on the part of financial institutions to collaborate on producing suitably balanced standard terms for cloud contracts in consultation with providers, obviously bearing in mind competition law restrictions.

In the middle or low value markets, choice and information are still limited, and many contract terms are still inadequate or inappropriate for users' needs; yet they may lack the bargaining power to force contract changes. Negotiations by large users with large providers, which have helped educate providers about users' issues such as privacy and security so that providers take due account of users' compliance concerns, will probably filter down to the middle market at least. This is because that market is potentially very large, and therefore attractive to providers. That may result in standard terms offered for mid-sized deals becoming more user-appropriate over time.

As for low value deals, action regarding inadequate contract terms may be needed by legislators or regulators, such as consumer protection or data protection authorities. However, legislators and regulators also need education regarding cloud computing technologies and business structures, so that laws and regulation enable cloud computing to be used in a balanced way so as to realize the potential economic benefits. Some of the current difficulties arise, not necessarily because contract terms are poor, but because data protection and financial services laws assume certain things that are not true in the cloud. In particular, current laws assume controllers' absolute control over processors, one-to-one relationships rather than one to many, dedicated instead of shared infrastructure, and processors who actively process data for controllers instead of renting out self-service resources.

With customized managed private cloud services on dedicated infrastructure, providers may be more flexible on contract terms. However, commoditized public cloud services on shared infrastructure are a very different proposition. They are cheap because they are standardized. One provider felt the biggest challenge was that users wanted the lowest price, but the highest specifications and features, such as location monitoring or audit rights. Forcing providers to accept more liability and incur the expense of upgrading their infrastructure, while asking them to maintain low commodity prices, does not seem an appealing proposition for providers, which may itself undermine market development. If one provider's infrastructure is not secure enough for personal data, users should choose another provider that does provide sufficient security.

In other words, rather than stipulating mandatory terms for commodity

cloud, a better course for policymakers may be to encourage a greater range of available cloud services (with different sets of terms) which users can assess, choosing the service best suiting their needs—whether cheap public clouds for data that are neither personal nor commercially confidential data, more expensive "personal data" clouds, or even more expensive, high security, auditable private or community clouds, such as sector-specific clouds for financial services or healthcare institutions.

Even mid-sized organizations, which may wish to process confidential or personal data in the cloud, are unlikely to have expertise to assess providers' security measures. Therefore, in order to enable consumers and small and medium-sized enterprises to consider and compare cloud services properly, work is also needed on industry standards and certifications, for sub-providers as well as direct providers, including standards on data portability and interoperability as well as security. Suitable standards and certifications, with provision for both self-certification and independent third party certifications, might then form the basis for laws that recognize appropriate certificates, trustmarks or seals as adequate for various compliance purposes.

In order for appropriate standards and certifications to be accepted by legislators and regulators, however, more openness and transparency are needed from providers. In particular, they need to explain more clearly and in more detail how data location relates to data security, including whether data may be secured against remote access by unauthorized persons even if located outside the European Economic Area or moved between different equipment, including data fragmentation and data structures. They need to spell out clearly the manner by which they are able to access users' data or monitor users' processing, if at all. They should perhaps also develop tools to, for example, enable users to verify accurately the locations of data and VM instances.

The increasing involvement of insurers in cloud is also relevant, as insurers may be better able to assess risks than smaller users. However, users may also need to consider actively insuring against providers' breaches, outages, data loss, and so on, checking that the coverage is appropriate.[97] One provider pointed out that, almost irrespective of how much liability providers accept, it was critical for users to understand cloud "layers" and data location.[98] Some smaller users have been contracting without understanding virtualization, the vertical supply chain or layering of providers; some even had no idea who pro-

97. Forty-three percent of users had insurance for business interruption due to the provider's disaster or data leak, but 37% did not know if they would be covered, although 65% of users expected their providers to cover these risks! *CIF3*, *supra* note 13, at 9.

98. As a consumer example illustrating the risks of ignorance regarding layers, users of the online backup service Backify, which is based on the Livedrive service, lost their data after a dispute between Backify and Livedrive. *See* Brid-Aine Parnell, *Punters Lose Backups in Cloud Storage Biz Spat,* THE REGISTER (Nov. 17 2011), http://www.theregister.co.uk/2011/11/17/livedrive_backify_dispute/.

vided the service. Ignorance of cloud structures may result in risks not being properly addressed. There is clearly also a need to help users climb the cloud learning curve. Users may for example need to consider which if any functions should be migrated to cloud and on what basis, such as starting with pilots only, conducting risk assessments, and implementing internal controls. They need to recognize that, quite apart from contract terms, they may need to take other practical measures, in particular pre-contractual due diligence and testing, encryption of data as appropriate, backing up internally or to another provider when using low-cost services without guaranteed backup, and post-contract monitoring.

In summary, while contract terms have been negotiated for larger deals, the small and medium-sized enterprise user market is unlikely to benefit in the short to medium term. While changes to providers' standard contract terms should filter down from large deals, and up from regulatory action regarding consumer and other deals, a multi-pronged approach may be the best solution, where all types of players are involved to encourage the development of a full variety of cloud services and contract terms priced at different levels, with standards and certifications to assist with legal certainty regarding compliance.