Legal Approaches to Management of the Risk of Cloud Computing Insolvencies

Rebecca Parry and Roger Bisson

KEYWORDS: cloud computing – insolvencies – contractual safeguards – public regulation

Cloud computing has revolutionised data handling in recent years in enabling the usage of computing resources, including for the storage of data, through flexible and on-demand services, often accessed through the internet.[1] One potential consequential challenge which has only been briefly touched upon previously is the containment of the impact of an insolvency in this area, as access to data, as well as the means of processing this data, may be significantly delayed or even lost upon the failure of a cloud service provider, 'CSP'. This is a matter of serious concern, both to businesses and consumers, as growing reliance on cloud computing technologies presents risks of an insolvency having a potentially systemic nature. This article represents an initial attempt to identify possible approaches to the threat of cloud computing insolvencies, suggesting a double layered approach in view of the significant risks for both businesses and consumers and with potential variations in scale and impact, with the potential for a 'too big to fail' scenario. Lying at the intersection of insolvency law and technological innovation this is an area which is as yet almost entirely unexplored.

Cloud computing arrangements give companies attractive possibilities regarding IT management, for example through outsourcing of elements. Cloud storage is almost instantly scalable and adaptable, one of the factors enabling users to achieve lower IT costs.[2] Significant savings can be made, for example since the need for companies to own hardware and pay associated running costs can be reduced and fewer specialist IT staff may be required. Software can be made more widely available through being offered for access through subscription. Cloud services therefore put advanced technologies within the reach of small and medium enterprises, for example, without the upfront cost that this would otherwise entail. Such potential savings are attractive in an economic climate which has generated a need for costs cutting, and this has thus fuelled the usage of cloud services.[3] Cloud computing also helps developers, as they can gain infrastructure without the expensive outlay that this would otherwise entail. It facilitates flexible working arrangements, including working from home and BYOD. It is estimated that by 2021, 94% of workloads and computing instances[4] will be processed by cloud data centres and the use of traditional data centres will decline.[5] The scalability of cloud computing also enables much faster processing and analysis of Big Data.[6] However, in spite

[1] For an overview of the benefits see European Commission, 'Unleashing the Potential of Cloud Computing in Europe' COM(2012) 529 final.
[2] Darrell M West, 'Saving Money Through Cloud Computing' (*Governance Studies and Brookings*, 7 April 2010) < https://www.brookings.edu/research/saving-money-through-cloud-computing/> estimating costs savings of 25% to 50% associated with cloud computing migrations.
[3] Various statistics are noted in Asokan Ashok, 'Four Trends in Cloud Computing CIOs Should Prepare for in 2019' (*Forbes* July 5, 2018). See for example the approach of the UK Government 'Cloud First' Policy, requiring public sector organisations to consider and evaluate potential cloud solutions ahead of other IT options.
[4] A term used broadly to describe many different applications, 'from a small lightweight SaaS application to a large computational private cloud database application'.
[5] *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper* (November 2018), text accompanying Figure 9.
[6] IAT Hashem, I Yaqoob, NB Anuar, S Mokhtar, A Gani, SU Khan, 'The Rise of "big data" on Cloud Computing: Review and Open Research Issues' (2015) 47 Information Systems 98.

of its many attractive features, cloud computing carries risks,[7] including the risk of provider insolvency, a matter that has not yet been significantly addressed either in literature on cloud computing[8] or on insolvency law and which is barely mentioned by service providers in promotional materials, nor highlighted in standard terms.[9] This issue is of considerable importance as the impact of an insolvency in this area is likely to be difficult to resolve[10] and can potentially be catastrophic for customers, including some with a public dimension, as outlined later in this paper. The risks that are consequently presented may also ultimately undermine competitiveness, in particular by damaging the attractiveness of smaller providers as business prospects, which may be regarded as riskier solvency prospects, leading to dominance by a very small number of suppliers.[11] In 2019 AWS had a market share of over a third, with another four cloud service providers, 'CSPs' having increasing market shares and a further four CSPs having substantial niche market shares[12] and the attentions of antitrust regulators have been piqued.[13] A far greater potential threat is presented by the insolvency of one of those suppliers, an insular vanguard[14] of a 'small number of large firms with increasingly worldwide presence'.[15] Such insolvency risks were noted by Lloyd's as being of potentially systemic impact[16] and giving rise to a possible 'too big to fail' scenario in which an approach which is merely reactive could lead to losses of data and productivity and give rise to significant costs.[17] One aim of this article is to consider whether a specific approach is required in respect of insolvencies in this area at state and international levels in order that an ex ante scheme

[7] Prashant Gupta, A Seetharamana and John Rudolph Raj, 'The Usage and Adoption of Cloud Computing by Small and Medium Businesses' (2013) 33 International Journal of Information Management 861 noted that in their study of SMEs there was a lack of confidence in the reliability of cloud service providers.

[8] The leading UK text, Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press, 2013) discusses insolvency only as grounds for the termination of a contract for cloud services. Timothy Morrow and others, 'Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud' Technical Report CMU/SEI-2019-TR-004 (Carnegie Mellon University, 2019), 14 addresses possible ways around being locked in to a bankruptcy CSP. Sean Marston and others, 'Cloud Computing - the Business Perspective' (2011) 51 Decision Support Systems 176, 182 mention insolvency as a risk but the matter is not discussed further. Sonal Dubey and others, 'SWOT Analysis of Cloud Computing Environment' (2017) Big Data Analytics 727 identifies cloud vendor shutdown as a 'very unstable situation' and identifies that the matter can be addressed through Service Level Agreements. As discussed below there are limits to the utility of this.

[9] For example, AWS addresses the impact of a customer's bankruptcy on the contract but not the impact of AWS's bankruptcy: <https://aws.amazon.com/agreement/>, para 6.1(d)

[10] European Telecommunications Standards Institute, *Special Report: Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing* (2016), 5.3.

[11] W Kuan Hon and Christopher Millard, 'Banking in the Cloud: Part 3 - Contractual Issues' (2018) 34 Computer Law & Security Review 595, 600 noting the view of one adviser that 'in five years, there will only be four providers: Amazon, Google, Microsoft and IBM'. For example, AWS is already the preferred cloud platform for 80% of enterprises for running apps or experimenting: Louis Columbus, 'Roundup Of Cloud Computing Forecasts And Market Estimates, 2018' (*Forbes* September 23, 2018).

[12] Synergy, 'Chasing Pack Gain Market Share in Q1 but Amazon Maintains a Clear Lead' (May 6, 2019), <https://www.srgresearch.com/articles/chasing-pack-gain-market-share-q1-amazon-maintains-clear-lead>, accessed 15 July 2019.

[13] Richard Waters, 'Department of Justice Opens Review into Big Tech's Market Power' (*Financial Times*, 24 July 2019).

[14] Roberto Mangabeira Unger, *The Knowledge Economy* (Verso, 2019), 1, 59.

[15] Above, 6.

[16] The dominance of a particular supplier can lead to a situational monopoly in respect of cloud infrastructure with potentially significant negative externalities. This combination of factors presents strong moral hazard risks: Shlomit Azgad-Tromer, 'The Infrastructure Ratchet Effect' (2018) 93 New York University Law Review 113.

[17] Lloyd's, 'Cloud Down, Impacts on the US Economy, Emerging Risk Report 2018' (Lloyds, 2018), <https://www.lloyds.com/news-and-insight/risk-insight/library/technology/cloud-down>: 'reliance on a relatively small number of companies has resulted in systemic risk for businesses using their services'

can be developed in place of such a reactive approach,[18] something which has been done in other sectors.[19]

This article presents an initial attempt to map the issues that can arise in the event of CSP financial difficulties and possible approaches to deal with them, since little detailed attention has been paid to this emerging issue previously.[20] This article in Part I will set out the cloud computing context, as different types of cloud services raise different issues and levels of risk in insolvencies, before potential impacts of cloud computing insolvencies are considered in Part II. Potential approaches to contain the impact of cloud computing insolvencies will then be set out. This article suggests a layering of private and public approaches to these insolvencies. Part III considers an initial private layer, where the risk of financial failure needs to be anticipated by CSP customers individually and the article will then consider steps that may be taken (primarily by business customers) to mitigate the risks of CSP failure through contract, as well as due diligence and contingency planning. However individual approaches give way to collective ones in the context of formal insolvencies and the impact of such proceedings will then be considered in part IV through theoretical framing, as well as considering in part V, primarily from a UK perspective, the impact of formal insolvency proceedings against a cloud service provider. Special considerations can arise in respect of CSP insolvencies, however, in view of their potentially strategic importance, giving rise to a possible need for a public-layer of regulatory intervention in a narrow range of cases and Part VI of the article will consider a number of normative solutions, building upon existing examples of regulatory intervention, as well as interdisciplinary literature.

I. Overview of risks presented by cloud computing insolvencies

In this section the risks presented by cloud computing insolvencies will be highlighted and categorised. Three elements arise from Renn's definition of risk, 'the possibility that human actions or events lead to consequences that affect aspects of what humans value',[21] namely, adverse outcomes, the possibility of occurrence and a formula to combine both. The focus in this section will be on identifying the possible adverse outcomes that may arise from cloud computing insolvencies. The possibility of occurrence, which depends inter alia on the vulnerabilities and resilience of systems,[22] is difficult to model since it may be presented by idiosyncratic events and these complexities are outside the scope of this paper.[23]

Cloud computing facilities fall into three types, with variations in the elements that remain under the management of the user and those that are outsourced and managed by the provider, although not

[18] Eva Hupkes, 'Insolvency – Why a Special Regime for Banks' (2003) 3 Current Developments in Monetary and Financial Law

[19] See the discussion in Part VI.

[20] See e.g. European Telecommunications Standards Institute, *Special Report: Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing* (2016) suggesting some basic approaches for retrieving data but noting that the issue in bankruptcy is 'hard to deal with'.

[21] Ortwin Renn, 'Three Decades of Risk Research: Accomplishments and New Challenges' (1998) 1 Journal of Risk Research 49, 51.

[22] Terje Aven, On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience (2011) 31 Risk Analysis 515.

[23] Renn, above n 21, 53. Potentially useful system analysis methods for the identification of cloud computing risks include deductive system analysis strategies which postulate systems failure and identify the possible causes, such as ageing components and/or improper installation, that can lead to this state. Methods such as fault tree analysis have been developed, see Liudong Xing and Suprasad V Amari, 'Fault Tree Analysis' in Krishna B Misra, *The Handbook of Performability Engineering* (Springer 2008), however there are limitations to the extent to which the human judgement on which they are ultimately based can be accurate and expert evaluations may not be available with sufficient rapidity: Franck Chauvel and others, 'Evaluating Robustness of Cloud-based Systems' (2015) 4 Journal of Cloud Computing 18.

all services fall neatly within these categories. It is necessary to provide a brief overview of each, as context for the discussion of risks which follows:

- Infrastructure as a service, 'IaaS', provides an instant computing infrastructure, consisting primarily of hardware provision for processing or storage, such as servers and real or virtual machines, together with virtualisation software to allocate hardware to particular customers. Examples are Rackspace and IBM Bluemix. This type of facility enables a user to avoid the costs of acquiring hardware while being in control of the operating system, middleware and applications. In the event of an insolvency the acquisition of a replacement infrastructure would be required, the difficulties of which are discussed in the next section.

- Platform as a service, 'PaaS', providing application hosting and deployment services, commonly acting as a platform for the development of software applications and commonly used by application developers, who offer the applications through the cloud. Such a service is attractive as it enables a developer to quickly develop an application without having to first set up and manage the infrastructure of servers, storage, network and databases. Here the user manages the application and data, while other elements, such as the operating system, middleware, virtualisation and hardware are managed by the provider. Examples of PaaS providers are Heroku and Salesforce's Force.com. In the event of failure of a PaaS provider, again a suitable replacement platform infrastructure would be required, the difficulties of which are discussed in the next section.

- Software as a service, 'SaaS', which provides internet access to software, normally on demand and on a subscription basis. Common examples are email and calendar services and data storage such as Dropbox. Apple's iCloud and Microsoft Office 365 offer advanced variations on this type of service. SaaS services include project management, collaboration and management tools and in some enterprises entire business processes are becoming cloud based, using services such as Basecamp and Trello. Under a SaaS arrangement the provider manages the underlying infrastructure, middleware, the software application and application data. The user connects to the application over the internet but will not always appreciate that they are using cloud-based services.[24] In the event of a SaaS failure the customer would lose access to the software and uploaded content such as data and the problems with preservation which arise will be addressed in the next section. A further problem would lie in continued use of the uploaded data as the acquisition of replacement software may be difficult, where it is not open source.

- Mention should also be made of differences in the means of deployment of cloud services, which can be via public cloud, private cloud, or a hybrid. Public clouds are operated by third parties for a variety of users on a pay as you go basis and hosted on the premises of the third party and, due to their nature, may be unsuitable for business critical or security sensitive information. Private clouds are operated by a single organisation for its exclusive use and therefore are low risk, although potentially used by many employees, and often hosted by the organisation on its own premises, although a private cloud can still be operated by a third party and off-premises. Hybrid clouds allow data and applications to be used across public and private clouds and commonly they will deploy the private cloud for business critical or commercially sensitive information and other data to the public cloud. Provider failures in the cases of hybrid and public clouds will then give rise to problems for large

[24] Patrick Ryan and Sarah Falvey, 'Trust in the Clouds' (2012) 28 Cloud Law & Security Review 513, 516.

numbers of users and the costs of preserving data may give rise to collective action problems, given a lack of coordinating mechanisms.

Cloud computing has revolutionised some areas of economic activity. To provide an example, competition in the banking market has been stoked by challenger entrants who have used cloud computing technologies to establish their operations. The competitive pressures that have been generated as a result, as well as regulatory market forces such as Open Banking, have caused longer-established banks, which carried out operational tasks in-house, to use new technologies including cloud services.[25] Cloud services are used for both operational activities, including elements of the core banking platform, and incidental activities, including IT services, threat assessment, accounting, marketing and other functions and are therefore increasingly important. A further practical example is the use of cloud technologies, including PaaS, to facilitate the use of blockchain technology by the marine insurance industry as proof-of-concept to replace paper-based industry practices.[26]

A failure could arise from a CSP entering insolvency proceedings or otherwise shutting down and ceasing to provide the contracted service, leaving customers such as banks and insurers without infrastructure and potentially without access to data and applications. The risks associated with cloud computing are not however confined to CSP insolvency, as sketched above. Another complicating factor is that the service that is provided may involve additional parties whose insolvencies could impact on the user,[27] as discussed in the next section, and there will not always be sufficient clarity about these arrangements to enable customers to fully anticipate the risks.

II. Potential impact of cloud computing failure

Cloud service provider insolvency should not be thought of as a remote possibility as providers can, and do, get into difficulties,[28] for example due to competitive pressures, poor strategy, an incident such as hacking or a natural disaster, or a lack of finance. Customers may find that they suddenly lose access to data, potentially facing a long and difficult retrieval process, a ransom situation under which they must pay sums to keep the service running while data is retrieved, or the loss of the data entirely. The outage may potentially threaten the user's business relationships with its own customers. Users of technology will be familiar with the frustrations and disruptions of interruptions of service. Even temporary outages can wreak havoc[29] and a longer-term outage due to an

[25] Capco Advertorial, 'Cloud: the Heart of the Digital Banking Revolution' (*Raconteur*, 2 June 2019) https://www.raconteur.net/sponsored/cloud-the-heart-of-the-digital-banking-revolution.
[26] Emmanuelle Ganne, *Can Blockchain Revolutionize International Trade?* (World Trade Organization 2018), 55.
[27] David S Caplan, 'Effects of bankruptcy of a cloud services provider', American Bar Association, Annual Meeting San Francisco, California, August 2010 <http://ftp.documation.com/references/ABA10a/PDfs/3_3.pdf>.
[28] See Cesare Bartolini and others, 'Cloud Providers Viability' (2018) 28 Electronic Markets 53. An example is Nirvanix, which filed for US Chapter 11 bankruptcy protection in 2013 and gave customers two weeks' notice before closing down. Even such a small time window may not be available in all future cases. Other cloud providers which have gone out of business are Megaupload and MegaCloud, while 2e2 is an example of a UK cloud provider which went into administration, briefly discussed in W Kuan Hon and Christopher Millard, 'Banking in the Cloud: Part 3 - Contractual Issues' (2018) 34 Computer Law & Security Review 595, 600.
[29] Mohammad Reza Mesbahi, Amir Masoud Rahmani and Mehdi Hosseinzadeh, 'Reliability and high availability in cloud computing environments: a reference roadmap' (2018) 8 Hum Cent Comput Inf Sci 20, identifying a lack of reliability of cloud services as a 'major issue. Brett Snyder and others, 'Evaluation and Design of Highly Reliable and Highly Utilized Cloud Computing Systems' (2015) 4 Journal of Cloud Computing Advances, Systems and Applications 11 estimated losses of $285 million due to cloud service

insolvency can potentially be catastrophic in terms of reputational damage, as well as economic losses. Those relying on public cloud service providers are particularly vulnerable.[30] One risk is that a 'run on the banks' scenario may potentially arise.[31] This situation would result from damage to the reputation of the CSP prompting customers to withdraw their data. The potential impact of the failure of a service provider is therefore a risk that must be considered, not only through prudence in contracting and in systems design, but also arguably from a regulatory perspective, as discussed in Part VI. The risks presented to cloud customers can be grouped in three main categories.

Risk 1, no loss of data but no means to process it.

As indicated, the challenges in the event of provider failure in each of the above cases will be to find an alternative provider. Particularly great issues will arise in respect of PaaS and SaaS where a business has become reliant on 'proprietary non-standard data formats and application logic'.[32] The task of replacement may be particularly difficult in respect of services that are offered using Artificial Programming Interfaces, commonly termed 'APIs', to enhance their capability. Applications which rely on artificial intelligence and machine learning may be irreplaceable. In contrast, where services are based on open source programmes the task of replacement will be more straightforward.

Risk 2, no loss of data but portability is difficult

The sourcing of alternative providers is only one aspect of the problem and greater challenges are presented by the migration of what is likely to be a high volume of data to a new provider. Large cloud computing infrastructures involving exabytes of data may be difficult to move between providers in a short space of time.[33] The impact of the bankruptcy of the service provider can be devastating for the user's business, in particular in cases where the bankruptcy happens suddenly, and no means of continued access can be arranged, either at all or at a viable cost. The tensions between the interests of creditors and the interests of customers that the difficulties of data transportation can give rise to in an insolvency will be explored later in this paper.

Another aspect of cloud computing failures that makes the retrieval of data difficult relates to the complexity of the arrangements, which can often involve different levels of service.[34] Rather than being stored on a single device in one location, cloud computing services may be based on a chain of

---

downtime based on 7.74 hours of unavailability per service per year. For a critical overview of cloud service provider reliability see Maurice Gagnaire and others, ' Downtime Statistics of Current Cloud Solutions' (*International Working Group on Cloud Computing Resiliency*, June 2012), <https://iwgcr.files.wordpress.com/2012/06/iwgcr-paris-ranking-001-en1.pdf>.

[30] Public clouds also present greater risks of isolation failure, a risk that arises where processing capacity is shared and one user may have an impact on another.

[31] European Network and Information Security Agency, 'Cloud Computing, Benefits, Risks and Recommendations for Information Security' (December 2012), p 19. As noted in Part V the moratorium in administration can potentially help to contain the exodus and see also the contractual restrictions discussed below.

[32] European Network and Information Security Agency, 'Cloud Computing, Benefits, Risks and Recommendations for Information Security' (December 2012), p 17.

[33] Robust technology is being developed to this end: 'How Amazon Uses Explosive-Resistant Devices To Transfer Data To AWS' <https://www.youtube.com/watch?v=H3_ZqnqLyVo&feature=youtu.be>, accessed 24 July 2019. This technology, AWS Snowball, can transfer data at a rate up to 1 Tb/s, allowing 100PB capacity to be filled in less than 10 days: <https://aws.amazon.com/snowmobile/faqs/>, accessed 24 July 2019.

[34] For example, the PaaS provider Heroku, often used for application development and deployment, and Netflix, the media company, which provides software to view its content on a SaaS basis, are both built on Amazon Web Services IaaS. Layering presents challenges from a security perspective also: Syed Hussain and others, 'Multilevel classification of security concerns in cloud computing' (2017) 13 Applied Computing and Informatics 57-65.

services provided by a variety of parties, with the result that different insolvencies among the parties will raise different issues. For example, the user may have entered into a contract with a SaaS provider using a broker as an intermediary. Unbeknown to the user, the SaaS provider may be using external PaaS services and the PaaS provider may be operating using IaaS provided by third parties, who in turn may be using facilities that are shared under a co-location arrangement, for example in a data centre.[35] Each link in the chain presents a risk of failure that can disrupt the user's access to data, software or technical support.[36] A lack of clarity for the user as to which services have been outsourced can present problems if attempting to retrieve data in the event of the failure of the cloud supplier.[37]

Portability issues can also arise in the period leading up to the insolvency. Service providers have incentives for business reasons to make migration to another provider difficult. Many providers limit the volume of data and application code that can be withdrawn during a specific period and there is a risk of some customers being locked in temporarily under the terms of their service contract. Such restrictions are to an extent applied in the collective interest, as a sudden migration could exacerbate otherwise temporary problems of the service provider, leading to its failure and accelerating the occurrence of consequential problems for customers.

Risk 3, loss of data

Issues can arise in relation to the security of the data[38] and the availability of the data, since the user may not be in full control of the data under a cloud service arrangement. The prospect of a loss of data can be anticipated by customers to some extent, through backups, although the backing up of current data, rather than a snapshot at a particular time, adds difficulty. It is notable that the potential impact of a cloud service provider failure could affect great numbers of customers in significant ways, particularly where a situational monopoly arises, as discussed in the fourth section.

Having reviewed the types of risk that are presented by cloud computing insolvencies, the next section will consider steps that customer may take to minimise the risk of disruption to their businesses in the event of CSP insolvencies, as well as the limitations of these approaches.

III. The private, contractual, layer of protection and its limitations

As in other contexts, the risk of insolvency can be addressed in several ways, preferably by private legal instruments, particularly by contractual arrangement between the parties, as well as contingency planning. Admittedly this is an approach which has significant limitations. Most cloud services will be provided under the CSP's standard terms and, as discussed below, these are likely to offer little benefit in an insolvency. Although more effective protections can be included in bespoke contracts, the availability of this protection is likely to be limited to large business customers as bespoke protection is beyond the bargaining power of most consumers and many MSMEs. Regarding negotiation, large scale providers are likely to present a lower risk of sudden shutdowns, for example, but smaller providers may provide a more bespoke service. Some strategies will depend on the level of bargaining power possessed by the client, which may be higher where a

[35] See further W Kuan Hon and Christopher Millard, 'Banking in the Cloud: Part 1 – Banks' Use of Cloud Services' (2018) 34 Computer Law & Security Review 4, 6.
[36] I Tasevski, 'Business Continuity in Cloud Computing' Tilburg University thesis 14 December 2014.
[37] European Network and information Security Agency, 'Cloud Computing, Benefits, Risks and Recommendations for Information Security' (December 2012), 23.
[38] Mohamed Almorsy, John Grundy and Ingo Muller, 'An Analysis of the Cloud Computing Security Problem', Proceedings of the APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010, arXiv:1609.01107 [cs.SE]; K Zetter, 'Diginotar Files for Bankruptcy in Wake of Devastating Hack' (*Wired.com*, 20 September 2011), <https://www.wired.com/2011/09/diginotar-bankruptcy/>.

smaller provider is the other contracting party. Some organisations will have higher bargaining power.[39] For example the pan-European data network Geant has a list of requirements that prospective cloud service providers must meet, including specific provision for insolvencies, as discussed below. Even for those who can benefit from a bespoke contractual approach there are limitations to the protection that contracting can provide, as will be discussed further below. Given the lack of access to contractual protections for many, and the limitations of the protection in cases where it is agreed, there may potentially be a need for regulatory intervention in exceptional cases where these private arrangements prove insufficient or non-existent, affecting customers on a wide scale, as discussed in Part VI. This section will consider the limitations of contractual approaches that businesses may adopt, based on service level agreement terms and bespoke contract terms such as software escrow and step in rights.

Although protection against the consequences of CSP failure is a matter for each direct customer, the most effective safeguard is in exercising prudence as to whether to enter into an arrangement with a CSP in the first place,[40] since otherwise risk may be difficult to contain contractually, for reasons which will be discussed, especially by MSME and consumer users. Such prudence should be combined with due diligence in entering into a service agreement, as well as contingency planning regarding the backing up of information and diversifying the CSPs that are used. In anticipation of CSP insolvency risk, it is advisable for a customer to identify possible alternative services that could be employed in the event of service provider failure, as well as means to recover the data, particularly if a high volume of data is involved.[41] Contingency planning is important as there are limitations to the extent to which a contract with a service provider can assist in the event of insolvency, as will now be outlined.

Standard terms of service provision

Cloud services will be the subject of service level agreements comprised of standard terms that may guarantee an amount of service uptime,[42] where direct customers may be reimbursed for periods of unavailability, as well as establishing clear delineation between the ownership of the cloud service infrastructure and the ownership of information stored by the CSP to ensure that the data belonging to direct customers or their customers does not form part of the CSP's bankruptcy estate.[43] However, these agreements may not provide significant protections to direct or indirect customers of the CSP in the event of an insolvency. The standard terms of service providers are likely to

[39] Large organisations may place significant restrictions on liability, for example: Timothy J Calloway 'Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: a Perfect Storm' (2012) 11 Duke Law Technol Rev 163.

[40] Cesare Bartolini et al, 'Cloud Providers Viability' (2018) 28 Electronic Markets 53 suggest how viability may be modelled. Garm Lucassen, Kevin van Rooij and Slinger Jansen, 'Ecosystem Health of Cloud PaaS Providers' International Conference of Software Business 2013, Software Business, from Physical Products to Software Services and Solutions 183 discusses the assessment of PaaS providers. Edward S Dove and others, 'Genomic cloud computing: legal and ethical points to consider' (2015) 23 European Journal of Human Genetics 1271–1278 discuss the issues involved in genomic research. There are, however examples of CSPs that have failed despite previously having records that would have satisfied stringent due diligence checks, with 2e2 given as an example.

[41] Timothy Morrow and others, 'Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud' Technical Report CMU/SEI-2019-TR-004 (Carnegie Mellon University, 2019), 14.

[42] Simon Bradshaw, Christopher Millard and Ian Walden 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services' (2011) 19 International Journal of Law and Information Technology 187, 214-215.

[43] Calloway, above n 39; Cesare Bartolini, Cristiana Santos and Carsten Ullrich, 'Property and the Cloud' (2018) 34 Computer Law & Security Review 358.

contain significant limitations on liability,[44] and, even if damages are payable, such a personal claim may not be of much value in an insolvency, where secured claims are likely to take the bulk of any returns to creditors. It is also notable that cloud computing standard terms often do not contain express provision for insolvency, in contrast to common standard terms in outsourcing agreements.[45]

Bespoke contractual protection

There are various strategies that can be adopted, with sufficient bargaining power, to enable a direct customer to recover both their own data, and their customers' data, in the event of CSP insolvency. The terms of the CSP service contract can expressly constrain the ability for the CSP to gain rights over customer data, particularly when such data is being produced using processing capacity and availability provided by the CSP under the service contract, potentially giving rise to proprietary claims. Alternatively, a 'captive insurance' entity may be used to underwrite the performance of a CSP agreement. Such prior agreements may also protect customers from being held to ransom by insolvency practitioners as discussed further below. The European Telecommunications Standards Institute emphasises the importance of prior work by clients before entering into service agreements and recommends the inclusion of a term setting out the legal consequences of the termination of the service contract in involuntary circumstances, including a contingency plan where services suffer unplanned outages, and plans for the handling of data migration and data security.[46] For example Geant's terms include a requirement for data to be accessible for at least three months in the event of a service provider declaring bankruptcy.[47] Monitoring can provide a further safeguard and a bespoke agreement may require regular reports on the financial status of the service provider[48] or early notification of potential financial difficulties,[49] although such a term might be difficult to enforce.[50] High standards will be expected by regulators of some sectors. For example, the Financial Conduct Authority requires that services be set up so as to enable the rapid return of firm deposits and client assets.[51]

However, even a carefully crafted contract regarding exit options and backups may fall into difficulties upon the insolvency of the CSP[52] and, as noted, a contract which provides a high level of service provider liability in the event of service failure may only give rise to a personal claim in the

[44] W Kuan Hon, Christopher Millard, Ian Walden, 'Negotiating Cloud Contracts: Looking at Clouds from both Sides Now' (2012) 16 Stan Tech L Rev 79, 92-3.
[45] See e.g. Practical Law Company and Simon Jones, 'Outsourcing Agreement: Long Form' < https://uk.westlaw.com/0-202-4551>. Accessed 28 November 2019.
[46] European Telecommunications Standards Institute, 'Special Report: Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing' (2016), 5.3.
[47] Geant, 'GN3plus Support to Clouds Terms & Conditions Requirements for Cloud Service Providers, Draft #3.2, 2.iv' < https://www.geant.org/Services/Connectivity_and_network/GTS/Documents/GN3Plus_SA7_Requirements%20DRAFT.pdf >, accessed 3 April 2019.
[48] Michael R Overly, 'Drafting and Negotiating Effective Cloud Computing Agreements' (*Lexis Practice Advisor Journal*, 30 November 2015).
[49] Such terms may have implications in relation to the twilight zone of insolvency, effectively implying much greater foresight obligations on members of the CSPs board.
[50] Cyrus A Morton, 'Mitigating Risk in Cloud Computing Agreements' (1 July 2014) <https://www.robinskaplan.com/resources/articles/mitigating-risk-in-cloud-computing-agreements>.
[51] Financial Conduct Authority, 'FG16/5: Guidance for Firms Outsourcing to the 'Cloud' and other Third Party IT Services'. See also European Banking Authority, 'Final Report, Recommendations on Outsourcing to Cloud Service Providers' EBA/REC/2017/03.
[52] I Tasevski, above n 36, 42-43, noting that data may be backed up with the insolvent service provider, rather than a third party, and also even if the data is backed up with a third party, the insolvency may hamper the effective performance of the backup system.

event of insolvency[53] that is likely to result in low returns to the CSP's customers and creditors in the event of insolvency. Even if a customer is able to recover their data, future access to and use of the data may depend on the continued availability of proprietary services. Complications may also arise from a cross-border insolvency perspective as different aspects of the service may have been provided by different parties in different countries.[54] Where insolvency proceedings are opened in one country it does not follow that the proceedings and the duties and obligations that flow from them will be recognised and respected by actors in cyberspace[55] located in jurisdictions each with their own approach to collective proceedings, and proprietary claims.

Better bespoke protection in the event of a SaaS insolvency may be provided by a software escrow arrangement. These multilateral arrangements developed so that software source code and related documentation would be held and maintained by an agent in an escrow account with tightly controlled access to the source code to protect trade secrets and intellectual property. The software will only be released to the licensee upon the occurrence of a triggering event, which could include the bankruptcy of the supplier. An escrow arrangement therefore provides potential reassurance to the customer regarding continuity of access to and ongoing maintenance of the software needed to access and use customer data. However, cloud computing presents an additional challenge in the context of a SaaS provider as failure presents the need for rescue and maintenance of not only the source code for any such SaaS platform but also other features of the cloud environment, such as the executable software, infrastructure configuration and, particularly, customer data, that is used to supply the SaaS services. The service provider might provide periodical or even real-time copies of the application and data. Some escrow providers have developed services to meet the cloud market, enabling a user's entire cloud environment to be stored. An alternative is for the supplier to provide regular backups or for a backup to initiate in the event that concerns arise regarding the supplier's finances.[56] In the absence of such arrangements, both the direct customer and any indirect customers may suffer an interruption in availability of the software upon bankruptcy of the provider; however, even where such an arrangement does exist there may be difficulties for both direct customers, or any indirect customers, as third parties to any such escrow arrangement, in enforcing the contract to gain access to the source code. This will particularly be so if there is a clause enabling the escrow agent to terminate the contract upon the bankruptcy of the cloud provider.[57] Tasevski suggests the use of a special purpose vehicle to act as escrow agent.[58] Such a measure is not as necessary however where open source software is involved.

A further term which might be included in a bespoke service contract would allow step in rights, a common power in outsourcing agreements, to be used. Such rights can, for example, entail an arrangement to be made directly between the SaaS customer and the hosting service provider if the provider of SaaS services were to become insolvent. In this eventuality the SaaS customer would take over payment obligations. However, such an arrangement may not enable the customer to

[53] The issue of whether a proprietary claim can be asserted is considered further below.
[54] It is beyond the scope of this paper to consider the complexities that would arise in such a case. It would be clearly desirable for office-holders to cooperate to minimise the impact on customers but, as noted elsewhere in this paper, there is likely to be a tension between the interests of cloud service customers and the interests of other creditors and this tension is potentially increased in a cross border case if, for example, cloud service customers are located in one jurisdiction while other creditors are located in another.
[55] Chris Reed, 'Why Judges Need Jurisprudence in Cyberspace' (2018) 38 Legal Studies 263.
[56] Martin Sloan, 'Escrow for Cloud and SAAS Services' <https://brodies.com/blog/ip-technology/escrow-cloud-saas-services/>, accessed 28 November 2019.
[57] Under US law and possible UK law reforms such a term would be contrary to the ipso facto rule against contractual termination on grounds of insolvency.
[58] I Tasevski, above n 36, 50-51.

gain access to the source code for the SaaS services and there is a risk that the office holder could withdraw the license to use the software.[59] Moreover, both the grant and enjoyment of such rights may not be straightforward in a cloud computing environment, with shared infrastructure, staff and third-party technology.[60]

Louwers notes that the splitting of copyright to the software has been suggested as a possible bespoke solution where a SaaS provider becomes insolvent,[61] although he also highlights various problems, including that a cloud service provider may be reluctant to part with a share of the copyright. It is also notable that this solution may be difficult to implement in practice where there are numerous users of the same software, and any effective distribution of intellectual property rights to a CSP's customers on bankruptcy has the potential to undermine any attempt by the office holder, to maximise the value of the service provider's intellectual property assets and goodwill. Again, a tension between the interests of creditors and the interests of CSP customers is noticeable.

Having outlined the limitations of standard terms of CSPs as well as the potential for bespoke contractual arrangements to minimise the risks of CSP insolvencies, and noted the limitations of each, the next sections will consider the approaches in insolvency. Initially it will consider how such cases might be approached from a normative insolvency perspective, before examining the insolvency procedures that are available under UK law, as an example of the formal insolvency laws that can apply in the event of CSP insolvency. It will be demonstrated that a range of approaches may be needed in view of the differing levels of impact of CSP insolvencies and, ultimately, that there is a need for international-level approaches.

IV. Normative insolvency framework

Theories of insolvency law under early normative distributional frameworks characterised such collective proceedings as addressing a common pool problem, regarded the role of the law as being to maximise the value of this pool in the interests of creditors, in their capacity as claimants of a pecuniary sum.[62] A focus solely on the interests of such creditors could potentially lead to a hasty closure in the interests of preserving the pool and enabling them to quickly cash out but such an approach can be rejected as insufficiently nuanced in relation to cloud computing insolvencies,[63] where a monetary claim is likely to be of little value to cloud service customers whose principal interests lie in access to data, particularly acutely in the case of business critical data, or the proprietary platform or infrastructure on which their business depends, and for which the market

[59] Ernst-Jan Louwers, 'Continuity in the Cloud: New Practical Solutions Required, an Inventory from a Dutch Perspective' (September 2013), available at <https://louwersadvocaten.nl/app/uploads/2016/08/louwers__ernst-jan_continuity_cloud.pptx.pdf>, accessed 20 February 2019.
[60] Sue McLean, 'Step-in to Reality: How to Ensure Effective Outsourcing Step-in Rights' <www.computerworlduk.com/it-management/how-ensure-effective-outsourcing-step-in-rights-3639897/>.
[61] Ernst-Jan Louwers, above n 59.
[62] Thomas Jackson, *The Logic and Limits of Bankruptcy Law* (Harvard University Press, 1986). This influential theory, which offered the first comprehensive normative framework for the discussion of bankruptcy laws has been the subject of much debate in subsequent years. See e.g. 'Bankruptcy's New and Old Frontiers' (2017-2018) 166(7) U Pa L Rev 1571 et seq. Nonetheless, the maximisation of returns to creditors is commonly regarded as one of the overriding objectives of corporate insolvency law, such as in Kristen van Zwieten, *Goode on Principles of Corporate Insolvency Law* 5th edn (Sweet and Maxwell, 2019), 2-01.
[63] More pluralistic approaches to bankruptcy policies are set out in sources including Donald Korobkin, 'Contractarianism and the Normative Functions of Bankruptcy Law' (1993) 71 Texas L Rev 541; Elizabeth Warren, 'Bankruptcy Policy' (1987) 54 University of Chicago Law Review 775; Rizwaan Jameel Mokal, *Corporate Insolvency Law Theory and Application* (OUP, 2005).

may be unable to offer a replacement.[64] More recently it has been recognised that a creditor's bargain model, based on a hypothetical bargain to underpin its system of asset distribution, fails to acknowledge the extent to which those affected by an insolvency can and do bargain,[65] both ex ante[66] and ex post[67] the insolvency. A contractual paradigm, where a greater role is played by agreements as a way of resolving corporate insolvencies, provides a more suitable approach for the resolution of cloud computing insolvencies, which may depend on an agreement for a managed close-down. It is in the interests of direct customers[68] and indirect customers of a company supplying cloud services to remain trading temporarily to enable customer data to be recovered and alternative service provision sought but customers' agreement to ongoing funding to enable this managed close-down may be needed, as discussed in the next section. There is, therefore, an inherent tension between the interests of cloud service customers and the ostensible interests of mere creditors, in the context of cloud service provider insolvencies; a tension that will be returned to.

A managed close-down in accordance with a contractual paradigm would suffice in many instances of CSP insolvency. However, in some instances a cloud service provider could be regarded as an example of what have been termed by Azgad-Tromer as 'Socially important non-financial institutions', [69] or 'SINFIs', the failure of which brings a risk of losses that may have a potentially great impact on individuals, going beyond the usual impact of insolvencies. A cloud computing provider may have a 'situational monopoly' in some circumstances, being the 'only relevant provider'. Azgad-Tromer gives several examples of cases in which taxpayer money has been used to rescue non-financial firms, such as hospitals and airlines. A recent UK example is the temporary financial aid given to an unnamed university.[70]

A situational monopoly may arise in the context of a cloud service provider insolvency because, as noted, data may not be easily accessible in the event of an insolvency and the recovery of the data will present greater complexities, since a replacement infrastructure, or compatible software, may need to be sourced and none may be available. In the case of SaaS it may be difficult to replace software needed to read data, for example. The loss of PaaS, IaaS or SaaS infrastructure may require replication of the platform as a whole where infrastructure is lost and this may not be practicable within a short timescale. As previously noted, cloud service customers can also find themselves locked in to particular services;[71] where, for example, data is held on a proprietary storage platform

[64] A position which is analogous to a claim for unique goods in contract law, which would give rise to a claim for specific performance, in view of the inadequacy of damages as a remedy. See e.g. *Behnke v Bede Shipping Co Ltd* [1927] 1 KB 649.
[65] David A Skeel and George Triantis, 'Bankruptcy's Uneasy Shift to a Contract Paradigm' (2018) 166 U Penn L Rev 1777.
[66] Through e.g. the provision of security.
[67] Through e.g. compromises and arrangements.
[68] Customers are excluded from the hypothetical creditor's bargain, except in so far as they are creditors. A customer may be regarded as a contingent creditor as they would have a claim if their data was lost or damaged. However, this claim is unlikely to be sufficient for the customer's needs, as discussed below.
[69] Shlomit Azgad-Tromer, 'Too Important to Fail: Bankruptcy Versus Bailout of Socially Important Non-Financial Institutions' (2017) 7 Harvard Business Law Review 159.
[70] Sean Coughlan, 'University given £1m bailout from watchdog' <https://www.bbc.co.uk/news/education-46223219>, 16 November 2018. Richard Vaughan, 'Three UK universities on the brink of bankruptcy and more reliant on short-term loans 'to survive'' <https://inews.co.uk/news/education/university-bankruptcy-reliant-on-loans-225766>, (*inews.co.uk*, 1 November 2018) reports significant use of bridging finance.
[71] Benjamin Satzger and others, 'Winds of Change: from Vendor Lock-in to the Meta Cloud' (2013) 1(1) IEEE Commun Surv Tutor 69; Robert H Carpenter, 'Walking from Cloud to Cloud: The Portability Issue in Cloud Computing' (2010) 6(1) Washington Journal of Law, Technology & Arts 1.

it may not be readable even if recovered because the customer does not have access to the software required for the data to be read.[72]

In the event of a CSP insolvency of significant scale and impact there may be a need for intervention by state agencies, at least as a coordinator of retrieval efforts, and international and domestic approaches in this regard are as yet lacking. Experience from other sectors shows that it is preferable to protect the functions of the institution rather than to prop-up the institution, for example with a bailout, in cases where no systemic risk is presented.[73] However the complex nature of cloud service arrangements may make such an approach difficult to emulate due to a lack of existing regulatory mechanisms at local and international levels, as addressed in Part VI. The next section will, however, consider how CSP insolvencies might be treated under current UK formal insolvency laws.

V. Impact of insolvency proceedings

A CSP which is in financial difficulties has various formal insolvency law options under UK law, giving the potential to enable continued trading by the company, or its underlying business and/or to manage the company's exit from the market through liquidation. These laws can provide a suitable framework for the managed close-down of the CSP which was suggested above as the most appropriate approach adopting a contractual paradigm.[74] However, the application of formal insolvency laws can be helpful, as such laws offer protections e.g. to prevent the repossession of equipment as well as a framework for dealing with creditors collectively and for compromise agreements to be reached by majority voting, as might be necessary under a contractual approach. A CSP insolvency is likely to present considerable difficulties for an office holder: such businesses often operate with high levels of automation and a limited staff base, and the volume of direct customer and, potentially, indirect customer enquiries may become overwhelming. The protections of the formal insolvency laws can be of assistance in facilitating a managed close-down, enabling customers to recover data and make alternative arrangements for services such as software. However, the continued operation of the CSP business will lead to costs that must be treated as an expense of the proceeding which will deplete the sums available for the provider's other creditors.[75] There is therefore a probable tension between the creditors with pecuniary interests in the insolvent entity who may favour a quick closure and the interests of customers, and creditors with principally executory interests, who would want a managed close-down. This section will explore this tension by reference to UK insolvency procedures but similar issues are likely to arise in other jurisdictions.

Liquidation

The insolvent CSP might enter liquidation and this procedure can be opened without the CSP's consent. This might provide a relatively simple and low-cost way to bring the affairs of the CSP to an

[72] Matthew Held, 'How to Protect your Business if your Cloud Provider Goes Bust' *Huffington Post* (12 April 2016).

[73] E Hupkes 'Protect Functions not Institutions' (2004) 9 The Financial Regulator 43 argues for the protection of functions rather than institutions even in cases of financial institutions in order that moral hazard issues associated with bailouts can be avoided. See e.g. The Bank of England, The Bank of England's Approach to Resolution' October 2017, p 8, where the favoured approach with smaller banks is for them to be allowed to fail, with compensation being provided to protected depositors.

[74] Many companies in financial distress of course find the use of collective insolvency laws unnecessary, in cases where creditors are sympathetic and there is no immediate risk of liquidation. In such cases negotiations with creditors on an individual basis can be an effective way to manage liabilities and avoid the expense and potential stigma of formal insolvency proceedings. See e.g. 'Vanessa Finch, Corporate Rescue: a Game of Three Halves' (2012) 32 Legal Studies 302, 307-309.

[75] Kristin van Zwieten, above n 62, para 6–26.

end and therefore might be preferred by creditors who are looking for quick resolution. It is unlikely to be in the interests of any cloud customer for the CSP to enter liquidation, however, given their likely need for a managed close-down. Although this procedure brings with it a stay on creditor claims, it is not designed as a vehicle for continued trading; liquidation is, primarily, a procedure under which a company's business is closed down and its affairs are brought to an end, on conclusion of which the proceeds of any remaining assets are distributed to creditors. There will be very limited scope for the existing management of the CSP to carry out any continued trading and they risk personal liability if doing so.[76] Control of the CSP will pass to a licensed insolvency practitioner who will be appointed as liquidator.[77] The liquidator has no power to continue trading except a far as this will be necessary for the beneficial winding up of the CSP,[78] a power that may be liberally construed.[79] Customers may have service agreements for pre-arranged capacity however nothing obliges an office holder to continue performance of contracts and those that the office holder does not wish to continue can either be disclaimed[80] or the office holder can cease performance whereupon the customer would become entitled terminate the contract on grounds of non-performance. In either case, only a personal claim for damages under the terms of the contract would arise against the insolvent entity; a claim that, by express limitation of liability, may be of little monetary value. Discontinuance of performance may be the last thing that a CSP customer would wish for given potentially irretrievable loss of data entrusted to the CSP. Whilst the customer will probably have property in the data[81] and may apply for a vesting order, data retrieval may be difficult and time-consuming, as previously noted. A further possibility is that the customer may be able to gain an order for specific performance however there is case law to suggest that such an order is inappropriate where a company is in insolvency proceedings.[82]

Restructuring

Although liquidation is unsuitable as a vehicle for continued operation under a managed close-down, while data is recovered, restructuring laws can potentially enable this. There are two main formal restructuring options, with the possibility of a third having recently been announced, that can provide a vehicle for the managed close-down of an insolvent cloud service provider, enabling data recovery by customers, or, in a case where the CSP remains viable, a restructuring to enable ongoing trading. Currently the simplest formal rescue option is the company voluntary arrangement, which

---

[76] IA 1986, s 103.

[77] This presents the problem of the liquidator of taking control of a technically complex business. However, under IA 1986, s 177 a special manager may also be appointed – such a person need not be an insolvency practitioner and they can be appointed, for example, to provide skills that the liquidator lacks, which could potentially be of benefit in a complex area such as cloud computing.

[78] IA 1986, Sch 4, para 5.

[79] *Re Wreck Recovery & Salvage Co* (1880) 15 Ch. D. 353 at 362 per Thesiger LJ.

[80] IA 1986, s 178, which applies only in England and Wales. A contract may be disclaimed if it is 'unprofitable' (s 178(3)(a)) and it is arguable that continuing obligations to perform cloud computing services could be regarded as such given their ongoing nature. See further *Re SSSL Realisations (2002)* Ltd [2006] Ch 610 where the critical factor was considered by Chadwick LJ to be that 'performance of the future obligations will prejudice the liquidator's obligation to realise the company's property and pay a dividend to creditors within a reasonable time', para 42. Notice of the disclaimer must be given to potentially affected persons, such as the cloud computing customers, so far as the office holder is aware of them: Insolvency (England &Wales) Rules 2016, r 19.3(1).

[81] See further Chris Reed and Alan Cunningham, 'Ownership of Information in Clouds' in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press, 2013) 142 et seq. It may be that the concept of 'property in data' might ultimately follow the GDPR concepts relating to duties to data subjects and data controllers, although this point would need to be established in case law.

[82] *Re Gough*, *Hanning v Lowe* (1927) 96 LJ Ch 239, [1927] B & CR 137; *Ullyott v Old Wharf Road (Grantham) Ltd* [2004] EWHC 82 (Ch), cited in John McGee (ed), *Snell's Equity* 33rd Ed (Sweet and Maxwell, 2018), 17-047.

typifies a contractual paradigm and enables an agreement to be reached between the company and its unsecured creditors, with the company remaining under the control of its directors, subject to supervision by an insolvency practitioner. This procedure can provide a vehicle for ongoing trading by a company, as it enables existing debts to be managed, but fresh liabilities will not fall under the arrangement. However, this procedure does not automatically bring the protection of a moratorium on creditor claims, and only small companies can apply for such protection.[83] Consequently, the proposal of a voluntary arrangement under this procedure will often have to be done while the company is in administration.

Administration brings with it the expertise of an administrator, with the company's existing management providing support. As noted, an insolvency practitioner is likely to have a steep learning-curve if taking on a company in this sector; and a managed close-down will take time.[84] Importantly administration provides the protection of a moratorium so the CSP is protected from winding up and legal acts that may harm the company in the short term for which permission of the court or an insolvency practitioner must be obtained beforehand. For example, creditors may otherwise seek repossession of goods that may be required to support managed data retrieval;[85] and landlords may seek repossession of company premises.[86] This moratorium commences upon the appointment of an administrator[87] and before that an interim moratorium applies during the appointment process.[88] This procedure would be potentially suitable for the managed close-down of an insolvent CSP as the moratoria will bring positive effects, notably in most instances[89] protection from winding up,[90] and unwarranted interference in the CSP's business operations at a critical time in its lifecycle..

A matter of concern for customers is the possibility that the moratorium may restrict their ability to access or retrieve their own, or their customers' data.[91] There has already been discussion in relation to the US automatic stay that arises under Chapter 11 that customers may be prevented from accessing or retrieving their data[92] and similar concerns may arise under a moratorium in administration which includes restrictions on legal processes in relation to the 'property of the company'[93] as well as legal processes against the company. [94] An initial point is that the data cannot be regarded as falling under the definition of company property, since the CSP normally gains no proprietary entitlement to the data under the terms of a service contract.[95] Therefore, the main impediment to data retrieval, at least through legal means, is the restriction on legal processes against the company, such as an application for possession. Moratorium protection is less effective

[83] IA 1986, s 1A and Sch A1, paras 2 and 3.
[84] The administrator can consent to leave some aspects of management in the hands of existing directors, however they may not in doing so evade their own responsibilities: IA 1986, Sch B1, para 64.
[85] IA 1986, Sch B1, para43.
[86] IA 1986, Sch B1, para 43(4).
[87] IA 1986, Sch B1, para 43.
[88] IA 1986, Sch B1, para 44.
[89] Limited exceptions are set out in IA 1986, Sch B1, para 42(4).
[90] IA 1986, Sch B1, para 42(2) and (3).
[91] Matt Hafter and Lauren Newman, 'Data in the Cloud: What if the Cloud Provider goes Bankrupt?' March 7, 2018 https://www.thompsoncoburn.com/insights/publications/item/2018-03-07/data-in-the-cloud-what-if-the-cloud-provider-goes-bankrupt
[92] Matt Hafter and Lauren Newman, above n 91.
[93] IA 1986, Sch B1, para 43(6).
[94] IA 1986, Sch B1, para 43(6).
[95] Matt Hafter and Lauren Newman, above n 91, discuss the matter in a United States context. A study by the Queen Mary, University of London Cloud Project found that CSPs did not typically assert claims to IP in information and content uploaded to the cloud: Christopher Millard, above n 8, 3.2.6.

against those with proprietary claims, since the moratorium is not an outright prohibition and permission to enforce such claims in spite of the moratorium will normally be given.[96] Nevertheless, the recovery of data held by a CSP, even where clearly the customer's property under the terms of the service contract, is likely to be difficult, given the intangible nature of data.[97] It is unlikely that the relationship between customer and CSP would be regarded as a bailment, as it is outside the scope of that legal concept, which only applies to tangibles,[98] nor is such a relationship likely to have been established by contract.[99] Customers would more likely be able to benefit from legal entitlements on the basis of copyright and database rights.[100] However, even if permission to pursue data recovery was obtained, recovery may not be logistically straightforward, as previously noted. These same difficulties mean that, in a case where the company is viable and is using the insolvency proceedings for temporary respite, the moratorium can help to prevent a rapid customer exodus, thereby avoiding further deterioration of the company's situation.

A proposal for a self-standing restructuring moratorium,[101] if legislatively implemented, would enable the existing management to remain in place and this can potentially be a good option for CSPs as it would avoid the costs of having to bring an insolvency practitioner up to speed on the company's business, in a technical industry with a low staffing base, as well as avoiding potentially damaging effects on staff morale. It is notable however that the proposed moratorium will only last, initially, for 28 days; a longer period may be necessary to enable the recovery of customer data for which an application for an extension may be required.

Data held to ransom

As noted, where the CSP enters insolvency proceedings it will be in the interests of customers for the company to continue to trade in order for data to be preserved, at least pending its customers finding alternative arrangements. However, a tension with creditors arises as ongoing trading leads to costs and the office holder is required to act in the interests of creditors.[102] As noted, a contractual paradigm would point to a managed close-down of the CSP under an agreement with the customers that are affected. This would in part address the tensions with creditors, since the costs of the close-down would not fall primarily on the estate. However, in this context the customers may find themselves effectively in a ransom situation. In the case of the data centre

[96] *Re Atlantic Computer Systems Ltd* [1992] Ch 505 542.
[97] *Oxford v Moss* [1979] 68 Cr App R 183; *St Albans City and District Council v International Computers Ltd* [1996] 4 All ER 481; David John Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (Hart, 2017), Ch 5.
[98] *Ashby v Tolhurst* [1937] 2 KB 242, 255; *Yearworth v North Bristol NHS Trust* [2009] EWCA Civ 37, [2010] QB 1 [48]. Nor, for the same reason, would the CSP be regarded as holding the content under a lien: *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281, [2015] QB 41.
[99] Christopher Millard (ed), above n 8, 3.2.7. There is insufficient space to consider the matter of ownership in detail in this context, not least because of the complexity of the dealings in many cloud computing arrangements. One issue is whether it is possible, for example, for there to be multiple proprietary interests in the same data at different levels of abstraction. If we refer to CSP1 as the insolvent CSP, CSP2 as CSP1's client, CSP3 as CSP2's client, and natural person NP1 as CSP3's client, if NP1 uploads data to CSP3 that it regards as proprietary to him or her, does that data become proprietary to CSP3, in additional to that of all CSP3's customers, and similarly CSP2, in the context of one or more proprietary claims against CSP1 for delivery-up of its data? Further, are CSP2, CSP3 and NP1 all entitled to make such proprietary claims simultaneously, or is NP1 restricted to a claim against CSP3?
[100] Christopher Millard (ed), above n 8, Ch 6.
[101] Department for Business, Energy and Industrial Strategy, 'Insolvency and Corporate Governance, Government Response' (August 2018).
[102] A liquidator has limited powers to continue trading and primarily is concerned with getting in the estate and distributing any realised proceeds: IA 1986, Sch 4. An administrator is required to act in the interests of creditors in general: IA 1986, Sch B1, para 3. A contrast can be drawn with CA 2006, s 172.

operator 2e2 the administrator is reported to have requested from customers almost £1 million in funding to keep the business running and enable customer data to be extracted in a secure way in a process that was estimated to require 16 weeks to complete.[103]

Legislative protection that would apply in the event of a ransom situation arising from the bankruptcy of a CSP has been provided in Luxembourg.[104] A law introduced in 2013[105] potentially enables the owner of data held by a bankrupt to reclaim that data. As might be expected, the application of this entitlement is restricted to cases where the data is separable from other assets. Even where this law applies, customers may still face difficulties.[106] As noted, the recovery procedures can result in delays, means of data transfer may not be straightforward and also an alternative platform must be identified, risk profiled[107] and engaged, so there may be significant disruption to the availability of data and this may impact significantly on customers' businesses. Difficulties will arise particularly in relation to SaaS platforms, as suitable alternative software may not be available, and the Luxembourg law provides no entitlement to possession or use of the SaaS software platform as configured if it is proprietary to the CSP or not otherwise separable from the SaaS software platform serving other customers as the law requires. A more powerful statutory power which could potentially be considered would enable SaaS software to be compulsorily acquired on the behalf of customers, and potentially their customers, collectively, although difficulties of enforcement and practical use could arise, including, for example, maintenance of the software sufficiently to enable it to be deployed.[108]

VI. A possible public layer of risk containment in cloud computing insolvencies

Given the limitations of contractual protection and possible data recovery issues, more powerful collective approaches might be developed for use in the event of an insolvency with a large public impact. Such a case might arise where a significant market provider of cloud services becomes insolvent, disrupting many businesses and leading to large-scale losses, even presenting systemic risk,[109] or where there is a public dimension, such as where a state agency has become reliant on cloud computing services.[110] Recent examples of cases having wide public impact have been seen in the banking and travel industries, which, like cloud computing, are both industries in which

---

[103] '2e2 Datacentre Administrators Hold Customers' Data to £1m Ransom' (*ComputerWeekly.com* 8 February 2013) <https://www.computerweekly.com/news/2240177744/2e2-datacentre-administrators-hold-customers-data-to-1m-ransom>.

[104] Although the law is wider than this, applying to intangible non-fungible goods more generally but expressed as having been introduced with recovery of data held by a bankrupt cloud provider in mind

[105] Luxembourg Code de Commerce, Art 567, briefly evaluated by Vincent Wellens, 'New Right to Reclaim Data from Bankrupt Cloud Computing Providers' (*International Law Office*, 28 June 2013).

[106] This protection would be usefully supplemented by the development and adoption of good practice standards for CSPs in relation to improvements in data portability and separation of tenant data; data volumetrics and cost estimates of a managed close-down.

[107] This step is likely to be the most time-consuming and ought to be performed with the same rigour and approach to risk as the original contracting process; as recommended by this article.

[108] Such powers would potentially need to be combined with stringent engineering management standards. The 'privacy by design' model, discussed in Ann Cavoukian, Scott Taylor and Martin E Abrams, 'Privacy by Design: Essential for Organizational Accountability and Strong Business Practices' (2010) 3 Identity in the Information Society 405, could provide a starting point for the prescription of standards, although greater practical and technical clarity would be required.

[109] As well as inconvenience and upset for customers of these businesses as well as customers of the cloud service provider.

[110] For example, in 2019 AWS hosts services for 4000 government agencies, per Bill Vass, Vice President of Engineering at Amazon Web Services:
<https://www.youtube.com/watch?v=H3_ZqnqLyVo&feature=youtu.be>, at 1:29, accessed 24 July 2019.

individuals place trust in respect of personal risk to themselves, their property or their data.[111] Particularly in the former instance the approach to insolvencies has given rise to much debate and the approaches taken can be considered for application in the cloud computing sector. There are further parallels with the crowdfunding sector, which is an emerging area with potential for insolvencies of wide public impact, impacting both on investors and borrowers and this paper will consider the regulatory approaches in these three areas. As an overview, there are two strands of regulatory approach in these three sectors: the preventative and the reactive. Much of the role of state institutions is geared towards this first strand of failure prevention, requiring that those involved in these sectors are on a sound financial footing with adequate risk controls.[112] In the event of financial distress a variety of approaches has been taken in the banking and travel sectors under the second, reactive, strand, including the protection of the functions of the distressed enterprise, as well as refinancing and reconstruction in some instances, as well as the provision of special procedures for handling insolvencies.[113] However it is likely that there will be limitations to the ability of individual states to provide effective protections in the CSP context and it will also be suggested that international approaches are needed.

Failure prevention

One notable difference in relation cloud computing relates to the first, preventive strand as there is virtually no state activity here. In contrast, the airline industry, the banking industry and, to a lesser extent, the crowdfunding sector are more tightly regulated. Entry to the banking sector is heavily controlled and banks are supervised, plus customer deposits are protected.[114] Similarly the airline industry is regulated domestically and internationally and customers already enjoy significant protections.[115] P2P crowdfunding platforms[116] must be authorised by the Financial Conduct Authority and are subject to safeguards discussed in the next paragraph.[117] In contrast the CSP industry presents regulatory difficulties inter alia due to location independence and it will be difficult for states to address these individually, a point which will be addressed at the end of this section. In common with airlines, CSPs may be obliged through contracts and market access to meet quality management standards.[118] However none of these quality management requirements relates to the financial state of the CSP. Beyond this, customers are, in general, solely responsible for the

[111] Patrick Ryan and Sarah Falvey, 'Trust in the Clouds' (2012) 28 Cloud Law & Security Review 513.
[112] For example, through the Bank of England Regulation Authority, in the case of banks. UK airlines are subject to licensing by the Civil Aviation Authority, which requires inter alia financial health, and an Air Operator Certification scheme relating to operational safety
[113] For example, Banking Act 2009, Part 2. In other sectors see for example Technical and Further Education Act 2017, Chapter 4.
[114] Under the Financial Services Compensation Scheme.
[115] Under the Package Travel Directive, ATOL Regulations 2012 customers are protected against the failure of the airline. Further protection is provided enabling costs to be recouped, although not immediately and in such cases the immediate costs of an alternative flight home would need to be found, although reduced price 'rescue fares' may be available. This protection arises under the Consumer Credit Act 1974, s 75, enabling claims for losses arising from a breach of the travel contract to be made against the credit card company through which the flight was booked. Passengers' own travel insurance may cover their costs arising from the insolvency. Those who paid for flights using credit cards may ask for the transaction to be reversed on grounds of non-provision of service.
[116] This is not the only type of crowdfunding platform but is focused on here for reasons of space.
[117] Financial Conduct Authority, 'Loan-based ('peer-to-peer') and investment-based crowdfunding platforms: Feedback to CP18/20 and final rules' (Policy Statement PS19/14) June 2019 <https://www.fca.org.uk/publication/policy/ps19-14.pdf>, accessed 28 November 2019. See also John Armour and Luca Enriques, 'The Promise and Perils of Crowdfunding: Between Corporate Finance and Consumer Contracts' (2018) 81 MLR 51 for a discussion of different regulatory approaches.
[118] Such as ISO 9001, ISO 27001 and PCI DSS. Airlines must observe quality management standards in respect of aircraft: <https://www.iso.org/ics/49/x/>, accessed 24 July 2019.

protection of their own data and that of their customers and for the logistics associated with the loss of facilities, such as software access, but there are limitations to the effectiveness of such approaches as discussed in Part III. Additionally, whereas the customers of airlines[119] and banks[120] typically benefit from compensation schemes, the losses and damages suffered by a CSP customer may be far greater than the value of the service provided, both in relation to the data itself and in relation to the availability of capacity to store, retrieve and manage the data; and any compensation due may not be available as soon as necessary to enable the preservation and data recovery.

The regulatory structure established in respect of P2P crowdfunding has variety of ex ante safeguards that will enable a failure in this sector to be managed and its impact limited. P2P platforms act as intermediaries between funders and borrowers. These platforms are required to have wind-down arrangements enabling funded agreements to continue even if the platform fails and a resolution manual to guide the resolution of the platform in the event of failure.[121] These safeguards can be identified as anticipating the resolution of failures without recourse to the public purse, since platforms are expected to maintain appropriate levels of capital and it is expected that the management of funding agreements during the wind-down arrangements will be financed from the income from the platform and that there should also be a guarantee that will cover the costs. [122] The approach of the protection of functions rather than entities is again identifiable, as it is expected that there should be an agreement with another firm that will take over the management of the P2P agreements in the event of the failure of the platform.[123] These approaches can be considered for CSPs but some potential problems can be identified. Arguably difficulties in applying a domestic approach to a supranational industry would arise.[124] A minimum capital requirement, for example, could easily be evaded through migration. A further difficulty is that CSP interfaces and the customer data under the management and control of the CSP may not be as readily severable as the platforms in the crowdfunding sector owing for example to issues already noted regarding data access and use depending on particular software. More positively, the concept of pre-planned wind-down arrangements and a resolution manual to provide guidance in the event of the failure of a CSP might be considered to be an example of good practice capable of emulation in the CSP context, given the likely difficulties faced by an insolvency practitioner in taking control of a CSP business, notwithstanding the costs of initial planning and preparation and ongoing maintenance. Any such rules applicable to a CSP context would, however, need to observe the technical, practical and economic drivers for CSP businesses.[125]

---

[119] Under e.g. the Denied Boarding Regulation, EU Regulation 261/2004.
[120] Under e.g. the Financial Services Compensation Scheme. In contrast this scheme does not apply to investors who have lost money through P2P crowdfunding.
[121] Financial Conduct Authority, 'Loan-based ('Peer-to-Peer') and Investment-based Crowdfunding Platforms: Feedback to CP18/20 and Final Rules' (Policy Statement PS19/14) June 2019, 2.29 et seq.
[122] *FCA Handbook*, SYSC 4.1.8C.
[123] *FCA Handbook*, SYSC 4.1.8C.
[124] David R Johnson and David Post, 'Law and Borders--The Rise of Law in Cyberspace' (1996) 48 Stan L Rev 1367.
[125] The preparation of pre-planned wind-down arrangements and the production of a resolution manual strictly in accordance with the crowdfunding model would invariably change the cost structure for IaaS providers, potentially undermining the viability of IaaS providers for certain types of business. For example, a provider may have a core network that is 'critical' to its business, complemented by an on-demand scalable network that responds to changes in demand and must be as cheap as possible. It follows that an insolvency protection regime may be best structured around identifying those 'functions' that are more, or less critical and providing for a cell-based entity that provides levels of protection for each; possibly forming multiple or many protective layers or tiers.

Reaction to failure

As far as the second, reactive, strand is concerned, state approaches to insolvencies vary. Attention will turn here to the banking and airline sectors, both rich in examples of strong emergency financial and institutional state intervention, as there has not yet been a P2P crowdfunding failure of the kind to require state intervention.[126] In the case of the banks,[127] the series of measures recommended by the review group, published in *The Run on the Rock*[128] included that taxpayers and depositors should be insulated from the risks of bank failure with depositor protection (the Financial Services Compensation Scheme) and clearer leadership and in subsequent years there were illustrations of a variety of approaches during the 2008 banking crisis. Within this sector there have been examples of the following 1) temporary liquidity support (Northern Rock, short term special liquidity scheme) 2) special insolvency restructuring laws, introduced in the light of the complexities that had been encountered following the insolvency of Lehman Brothers and to minimise disruption to the financial markets[129] 3) state investment (purchases of shares via the Bank Recapitalisation Fund in the cases of Royal Bank of Scotland, HBOS and Lloyds TSB), 4) state institutions for the protection of customers, notably the Financial Services Compensation Scheme. Both entities and functions have been preserved and it has been unusual for banks to be allowed to fail, although BCCI and Lehman Brothers are examples.

Approaches to airline insolvencies have been similarly variable.[130] International examples of state involvement have included 1) temporary liquidity support (bridging finance in the case of Air Berlin) 2) special insolvency restructuring laws, exemplified by the use of special restructuring laws in the case of Alitalia 3) state investment, also in the case of Alitalia and 4) the use of state institutions for the protection of customers, notably the use of state agencies to effect repatriation of stranded passengers in the failures of the airlines Monarch[131] and more recently Thomas Cook. Both airline cases are examples of the protection of functions rather than entities in a case where an airline has been allowed to fail. Monarch prompted a review which led to the formation of policies for the handling of future cases of failed airlines[132] and these policies can potentially provide a model for the handling of the future insolvency of a CSP.

The state agency effected passenger repatriation in the example of Monarch can be regarded as a rescue of functions and Monarch as an entity was left to exit the market. Monarch had entered administration in October 2017, leaving 110,000 passengers stranded abroad and a layering of approaches was evident. Some passengers held ATOL insurance, but many were without this and public intervention was considered necessary in cases where private arrangements had not been made, since more passengers required repatriation than the market could deal with.[133] This approach may be instructive in other cases of wide impact, including CSP insolvencies. This approach of picking up functions rather than bailing out Monarch may be contrasted with the bridging finance given to Air Berlin to keep running. However, it is notable that the costs per passenger of the Air Berlin approach were likely to have been lower, as it enabled existing capacity

[126] Failures of P2P lenders regulated by the FCA have included Lendy and FundingSecure.
[127] L Laeven and F Valencia, 'Resolution of Banking Crises: The Good, the Bad, and the uUgly' (IMF Working Paper) (Washington, DC: International Monetary Fund, 2010); Emiliano Grossman and Cornelia Woll. 'Saving the Banks: The Political Economy of Bailouts.' (2014) 47 Comparative Political Studies 574.
[128] House of Commons Treasury Committee, *The Run on the Rock* (Fifth Report of Session 2007–08).
[129] Investment Bank Special Administration Regulations 2011, SI 2011/245.
[130] Pietro Benintendi, 'Bankrupt in Europe: A Case Study of Three Recent Airline Insolvencies' (2019) 44 Air & Space Law 241.
[131] Airline Insolvency Review, chaired by Peter Bucks, *Airline Insolvency Review Final Report* (March 2019).
[132] *Airline Insolvency Review*, above.
[133] HC Deb 9 October 2017, vol 629, col 34.

to be used, rather than lying redundant as in the example of Monarch,[134] with state-enabled repatriation at a cost of £476 per passenger.[135] The managed close-down of the insolvent entity may therefore be preferable to functions being picked up by a separate entity, although the same approach was subsequently followed in the repatriation of customers of Thomas Cook, around 150,000 passengers at an estimated cost of £100 million.[136]

The review of airline insolvencies[137] commissioned by the UK Government following the Monarch failure sought to limit the need for government intervention and consequential demands on public resources. The report identified five principles: 1) that those who benefit ought to pay for their protection; 2) that risks should be allocated to those best able to manage and control them; 3) that market distortions should be minimised and UK airlines not be disadvantaged; 4) that there should be transparency for passengers as to the protection available and risks covered and compensation and repatriation should be done quickly; and 5) that the approach should be deliverable by the government with minimal legal risk. This report potentially gives a blueprint for how CSP insolvencies could be addressed while limiting the need for government involvement, even if the application of the principles identified in the report do not produce the same outcomes. The application of the principles led to a package of recommendations enabling a coordinating body, most likely the Civil Aviation Authority, to oversee the repatriation of passengers. Costs were to be met by a Flight Protection Scheme for the repatriation of passengers, to be coordinated by the Civil Aviation Authority and funded by airlines serving the UK market, at only a small cost to passengers, and this was therefore a system that would not require public funds. It also recommended means to keep airlines operating temporarily, including a new insolvency procedure, the Special Administration Regime, so that insolvent airlines could continue to operate flights temporarily for the purposes of passenger repatriation and the costs efficiencies of temporarily keeping the fleet flying, rather than the operation of charter flights for repatriation, could be captured.

These same principles and layered approach can arguably be applied in the context of CSP insolvencies and it is desirable that an infrastructure should be developed ahead of time to minimise the impact of likely failures:

> 1) It is for CSP customers to pay for their own protection. As noted, this is the starting point and preparation for protection is paramount, not merely payment for protection. As previously discussed, service agreements can include provision for insolvencies, although the utility of this approach is limited. The Airline Insolvency Review rejected a 'buyer beware' approach as insufficient.[138] Arguably the risks presented by CSP insolvencies require that a wider strategy be developed for use in the event of an insolvency presenting significant externalities, potentially systemic in nature.
>
> 2) Risks should be allocated to those best able to manage and control them. Costs would be expected to be borne by direct and indirect customers rather than the taxpayer. In the case of the airline industry it is proposed this would be achieved by the repatriation scheme being

[134] It is unlikely, however, that in cases where an airline is in administration, an administrator will wish to continue to operate flights, in view of possible liabilities and risks to reputation, as well as the costs of doing so: Kevin Pullen and others, 'Airline Insolvency Review' (*Herbert Smith Freehills*, 2019) <https://www.herbertsmithfreehills.com/latest-thinking/airline-insolvency-review>.
[135] Simon Calder, 'Air Passengers Set to Pay Levy of up to 50P in Case Airlines Go Bust' *Independent* (9 May, 2019).
[136] HC Deb 25 September 2019, vol 664, cols 688 and 713.
[137] *Airline Insolvency Review*, above n 131
[138] Ibid, 9.

funded by the airlines through a small levy per passenger departing from the UK. In the CSP context a levy could in theory be applied to cloud service providers based on the volume of data stored but such an approach might be difficult for any one country to operate as there may be no fixed location where data is stored[139] and an international approach may be preferable.

3) Market distortions should be minimised and local providers should not be disadvantaged. One issue which may again be noted in this regard is that efforts to regulate CSPs can be evaded by relocation. This points again to a need for development of an international approach, as addressed in the last paragraph of this section.

4) Direct and indirect customers should have transparency as to the protection available. Arguably greater awareness of the potential for CSP insolvencies can be generated, since these risks are not widely addressed by service providers and are potentially under-appreciated by customers throughout the supply chain.

5) An approach should be deliverable with minimal legal risk. As noted, in the CSP context risks arise from jurisdictional issues as well as the problems of retrieving data and sourcing alternative services.

The likely situational monopoly of some CSPs and their potential to impact on diverse customers in significant ways, including the prospect of a 'too big to fail' scenario, presents the possibility that a coordinated and specialised approach may be required, limited to the protection of the functions of the CSP for a limited time frame while customer data is retrieved and alternative services, if available, are sought, or the software of the CSP is acquired. In other contexts, specialist insolvency procedures have been developed and this is something that has been recommended in relation to airlines, but this solution would depend on political will and legislative time. Suitable approaches in the interim may be better achieved through private ordering.[140] Another recommendation in relation to the airlines was that a coordinating role can be provided by an agency, in the case of the airlines the Civil Aviation Authority but there is no equivalent body in the CSP context. This coordinating role can instead be performed by a private actor with specialist expertise who might initially act as an adviser to insolvency practitioners responsible for managing CSP insolvencies.

Arguably, however, a more ambitious approach is required as CSP insolvencies are potentially supranational in nature where the development of domestic approaches will be insufficient. International approaches would depend on consensus among states as well as the will of organisations who might drive forward a convention or other instrument.[141] As yet, supranational initiatives are lacking. Regulation of the CSP sector is kept under review by European Union agencies but remains primarily a matter for self-regulation at national level, aside from in relation to matters of broader concern, such as cyber security, data protection and consumer law. International institutions have paid some attention to aspects of cloud computing, through efforts which have

[139] This is an issue which also gives rise to difficulties in the context of taxation. Ron Saake and Mandana Malone, 'International Tax Issues and Cloud Computing' (*International Tax Review*, 23 January 2014) <https://www.internationaltaxreview.com/article/b1f9k1nm7djlfv/international-tax-issues-and-cloud-computing> accessed 13 December 2019.

[140] Steven L Schwarcz, 'Private Ordering' (2002-3) 97 Nw U L Rev 319, 326.

[141] In a different context such consensus and will has led to the agreement of The Cape Town Convention on International Interests in Mobile Equipment. This Convention may be regarded an example of an international instrument designed to address uncertainties in relation to assets without a fixed location. It provides greater levels of certainty issues in relation to the treatment in insolvency of registered interests in assets that are continually crossing borders.

been made in relation to matters including data protection and privacy. Given the potentially significant risk presented by CSP insolvencies there is a need for the development of preventative and reactive strands. As noted previously, a preventative approach would suffer potentially from a governance gap due to the potential for evasion through relocation to non-compliant jurisdictions, as in relation to evasion of corporate taxation.[142] To enable a reactive approach to CSP failure, funding could potentially be through a scheme similar to that which mitigates the impact of international oil pollution. In that example a compensation scheme is funded by entities who receive shipments of oil.[143] Following this example, a levy on cloud computing users could potentially be used to fund a scheme to enable the managed close-down of an insolvent CSP in a case where funding by the customers of the insolvency CSP is not sufficient.

VII. Conclusion

The risks of cloud service provider insolvencies are potentially significant, but they have not previously been considered in detail. Literature has merely highlighted the difficulties that such an insolvency would present but has not examined possible solutions in detail. This article represents an initial attempt at a roadmap for such solutions, aimed at the ex ante development of a framework for the handling of CSP insolvencies.[144] Although the starting point should be the incorporation of terms in service agreements, as well as due diligence and contingency planning, there are limits to the extent to which CSP customers, in particular consumer and SME customers, can protect themselves contractually, often through a lack of bargaining power and also through the weak position that the holder of a personal claim arising from breach of a CSP service contract will find themselves in in the event of CSP insolvency. The difficulties of data recovery in useable form in the context of some CSP insolvencies were noted as giving rise to a tension between the interests of customers who will want a managed close-down and the interests of creditors, who will wish to avoid the costs of this. This is an area which demands concern, given the potential for impact on a large numbers of customers, potentially including public bodies and financial institutions, in the event of a CSP insolvency, as well as the economic impacts of resulting outages and the attention which is now being paid to the possibility of a 'too big to fail' scenario. A basket of protections might be considered for the managed close-down of an insolvent CSP and in the short term this may require in particular the development of specialist professionals to coordinate cases and, proactively, the adoption of a best practice approach to preparation of wind-down arrangements and a resolution manual so that insolvency practitioners are provided with guidance in the event of a failure. In the longer term it is desirable for the coordinated resolution of CSP insolvencies to be on the agenda for states and more importantly international institutions and organisations.

[142] Kermal Dervis, 'Closing the Global Governance Gap' (*Project Syndicate*, 29 May 2019) <https://www.project-syndicate.org/commentary/digital-technologies-global-governance-challenges-by-kemal-dervis-2019-05>.

[143] Under the rules of the International Oil Pollution Fund, liability to compensate those who have suffered damage from oil pollution from a ship falls initially on the shipowner. The fund provides compensation in the event that there is an applicable exemption available to the shipowner, or if the shipowner is insolvent.

[144] We have focused on CSP insolvencies but note also the potential for insolvencies of cloud service customers, 'CSCs'. The CSP may remain under an obligation to continue supply of services to an insolvent CSC despite a term purporting to enable termination of the service contract owing to the characterisation of various information technology services as essential services under IA 1986, s 233(3)(f) and 233A.