Cloud Computing 2022

Contributing editors
Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston

LEXOLOGY®
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2017
Fifth edition
ISBN 978-1-83862-634-1

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Cloud Computing
2022

Contributing editors
Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston
Bryan Cave Leighton Paisner LLP

Lexology Getting The Deal Through is delighted to publish the fifth edition of *Cloud Computing*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston of Bryan Cave Leighton Paisner LLP, for their assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
September 2021

Contents

United States

Sean Christy, Chuck Hollis and Derek Johnston
Bryan Cave Leighton Paisner LLP

MARKET OVERVIEW

Kinds of transaction

1 What kinds of cloud computing transactions take place in your jurisdiction?

In recent years, there has been an explosion in the number and types of cloud computing transactions in the US. If cloud computing is broadly construed as the acquisition and purchase of computing power or software applications that are utilised remotely, then virtually every business entity in the United States, whether public or private, and virtually every governmental entity (including the US military) currently rely on and use some form of cloud-enabled service, or purchase some type of cloud-based computing resources to support their daily operations.

With that said, the most common and widely accepted forms of cloud computing transactions in the United States are the three types or categories of cloud computing transactions identified as the software as a service (SaaS) model, the platform as a service (PaaS) model, and the infrastructure as a service (IaaS) model.

Software as a service

The SaaS model is undoubtedly the largest of the three in the United States by revenue, due to its ease of deployment, cost-effectiveness and low maintenance charges. Indeed, in a very short period of time, this model of software licensing has become ubiquitous in the United States, and many American consumers license and utilise software applications on this basis without even knowing it. There are, by way of example, many everyday services such as Netflix and other streaming services, as well as many applications, such as Google Mail, that are based on cloud computing models. The same is true for US businesses, with the vast majority of enterprise resource planning (eg, HR, financial) and other common and niche business applications provided and consumed on a cloud computing deployment model.

While there are many different and often conflicting reports and projections regarding the size of the SaaS market in the United States and its rate of growth, all analysts agree that the SaaS market will grow wildly in the near future. According to KBV Research, the global SaaS market is expected to reach approximately $185 billion by 2024, with the North American SaaS market alone expected to grow at a compound annual growth rate of 19.9 per cent during the period from 2018-2024.

Infrastructure as a service

The second most significant form of cloud computing transaction in the United States, from a revenue perspective, is IaaS model. A recent IDC report determined that global revenue from IaaS services in 2020 was $67.2 billion. Once again, all analysts agree that the growth in this form of cloud computing transaction in the United States will not abate in the near future. KBV Research estimates the Global IaaS market will reach a market size of $89.9 billion by 2023, rising at a compound annual growth rate (CAGR) of 25 per cent during the period from 2017-2023. And while there is again no specific break out of the US IaaS market, KBV Research expects the North American IaaS market to grow at a CAGR of 24.3 per cent during the period from 2017-2023.

Platform as a service

The IDC report referenced above found that the total revenue derived from PaaS services in 2020, which are the third most widely-used cloud computing services in the United States, was $47.6 billion.

As we can see, by any estimate or measure, the revenue generated from cloud computing transactions is enormous and the trend toward cloud computing will continue unabated for the foreseeable future. Indeed, cloud computing has now become a mission-critical piece of operations for virtually any US business entity.

It should also be noted that in the United States each of the above cloud computing services may be deployed through public, private and hybrid cloud deployment models, depending on the business objectives, security concerns, scalability requirements, span of control and other concerns of the entity entering into the specific cloud based transaction. It is, nevertheless, much more common to see SaaS business applications deployed using a public model in the United States, given the scalability of public cloud deployments and the usage-based pricing often accompanied by these models, where the vendor hosts and manages the application in a multi-tenant environment.

Project JEDI

Finally, as for the most significant cloud computing transactions in the US in recent days, there is little doubt that the US Department of Defense's Joint Enterprise Defense Infrastructure acquisition (Project JEDI) continues to receive the lion's share of attention from both the press and the US public. As has been well-publicised, Project JEDI was an effort by the DoD to award a single cloud service provider virtually all mission-critical IT workload for the US military. The total value of Project JEDI was estimated to be $10 billion, and the prestige associated with winning the contract may well have exceeded the dollar value of the contract itself.

While the DoD initially awarded Project JEDI to Microsoft, Amazon Web Services (AWS) – Microsoft's principal competition for the contract – subsequently sued alleging, among other things, inappropriate political influence. After some protracted litigation, the DoD cancelled its $10 billion contract in July 2021, to the surprise of many, and has now announced a new contract that will include multiple cloud service providers, as well as AWS.

Active global providers

2 | Who are the global international cloud providers active in your jurisdiction?

Given the size of the US cloud computing market, most, if not all, of the global international providers are active in the US.

The largest international cloud infrastructure providers active in the US in 2021 are AWS, Microsoft Azure, Google Cloud, Alibaba Cloud, IBM Cloud, and Dell Technologies/VMWare.

In addition, companies such as Salesforce.com and ServiceNow are noteworthy for their cloud-based SaaS offerings.

The most widely followed and frequently cited industry reports on the principal cloud service providers, both by category and type of service provided and their respective market positions are prepared by Gartner Inc. These reports are available to Gartner Inc. account holders and through other third parties.

Active local providers

3 | Name the local cloud providers established and active in your jurisdiction. What cloud services do they provide?

The 'local' cloud providers in the United States are largely the same as the global international cloud providers. The principal cloud infrastructure providers are AWS, Microsoft Azure, Google Cloud, IBM Cloud and other players such as Oracle and Dell Technologies/VMware.

Some noteworthy SaaS providers include Salesforce.com, Microsoft, Adobe Inc, SAP and ServiceNow, Inc. Of course, there are smaller and more specialised cloud and SaaS providers in the United States, such as Rackspace and Workday.

The most widely followed and frequently cited industry reports on the principal cloud service providers, both by category and type of service provided and their respective market positions, are prepared by Gartner Inc. Gartner's reports are available to Gartner Inc. account holders and through other third parties.

Market size

4 | How well established is cloud computing? What is the size of the cloud computing market in your jurisdiction?

Cloud computing is well established in the United States. According to some analysts, on an annual basis the overall cloud computing market, ranging from cloud infrastructure providers to SaaS providers, currently generates over $100 billion in revenue in the United States alone. And the compound annual growth rate for this market has been well in excess of 25 per cent in recent years.

Going forward, the size of the overall cloud computing market is only expected to continue to grow at a breakneck pace, with some projecting the market to reach over $287 billion during the period from 2021-2025.

Impact studies

5 | Are data and studies on the impact of cloud computing in your jurisdiction publicly available?

There are many publicly available studies about the impact of cloud computing in the United States. The authors of these studies represent some of the more well-established educational institutions and technology and consulting organizations in the world, such as International Data Group (IDG), Gartner Inc., Deloitte and PwC, and MIT. Taken as a whole, these studies indicate that the growth in cloud computing will continue unabated for the foreseeable future. By way of example, the IDG study concludes that close to one-third (32 per cent) of total corporate IT budgets will be allocated to cloud computing in the near future. IDG also found that 92 per cent of organisations' IT environments are at least partially in the cloud today, as only 8 per cent stated their total IT environment was on their premises.

As corporations continue the transition to the cloud and away from legacy solutions, it is certain that the providers of legacy solutions will be negatively impacted and traditional models of collocated infrastructure and legacy IT outsourcing will continue to evolve to a managed cloud model.

POLICY

Encouragement of cloud computing

6 | Does government policy encourage the development of your jurisdiction as a cloud computing centre for the domestic market or to provide cloud services to foreign customers?

Yes. In fact, in 2019, the US government issued its Federal Cloud Computing Strategy, articulating the US government's overall strategy to accelerate and drive the adoption of cloud-based solutions for itself and its agencies. In that document, the US government confirms its view that cloud-based solutions, when properly implemented and overseen, can and do enhance mission and service delivery.

In addition, the US government has published various policies that, directly and indirectly, confirm the validity and use of cloud-based solutions in support of federal activities. For example, Third-Party Relationships: Risk Management Guidance establishes certain risk management principles for banking organisations that engage third party providers, including third-party cloud service providers.

Finally, there are a number of federal guidelines that identify specific security concerns raised by cloud computing solutions and that offer guidance on how federal agencies may generally mitigate these concerns when implementing cloud-based solutions. (See Security in a Cloud Computing Environment joint statement from the US Federal Financial Institutions Examination Council and Cloud Security from the US Cloud Information Centre.)

Incentives

7 | Are there fiscal or customs incentives, development grants or other government incentives to promote cloud computing operations in your jurisdiction?

To our knowledge, there are no specific fiscal or customs incentives, development grants or other incentives to promote cloud computing operations in the United States. That having been said, there are grants and incentives in the United States that promote technological investment more broadly and, therefore, the provision of cloud computing technologies as well. Further, large cloud computing service providers will often negotiate tax or other governmental incentives on a case-by-case basis with individual states as a condition of investment in those jurisdictions.

LEGISLATION AND REGULATION

Recognition of concept

8 | Is cloud computing specifically recognised and provided for in your legal system? If so, how?

In the United States, a cloud computing services contract is largely treated, from a legal perspective, like any other service or commercial contract. Accordingly, cloud computing services contracts are, in the main, governed by state (and not federal) law, with some federal overlay based on the subject matter of the specific contract.

The federal laws and statutes that are commonly implicated in cloud-based services contracts range from data privacy and security laws specific to financial transaction information, healthcare information and the like. These include:

- the Gramm-Leach-Bliley Act, which applies to financial services;
- the Health Insurance Portability and Accountability Act (HIPPA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which apply to protected health information;
- the Family Educational Rights and Privacy Act (FERPA), which applies to educational institutions and their vendors; and
- federal and state laws and regulations that apply generally to third-party service providers in given industries, such as:
  - third-party risk guidance for the financial services industry from the Federal Reserve, the Office of the Comptroller of the Currency (OCC), the Financial Industry Regulatory Authority (FINRA), the New York State Department of Financial Services (NYDFS), and other regulatory agencies; and
  - FERPA, which in addition to governing data privacy, also governs the scope of permitted outsourcing in higher education.

Governing legislation

9 Does legislation or regulation directly and specifically prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

Not specifically, no.

10 What legislation or regulation may indirectly prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

There are numerous federal and state laws and regulations that may indirectly impact the use of cloud computing applications and use cases. For example, there is a patchwork of federal and state privacy laws that may impact the application of cloud computing. At the federal level, the Gramm-Leach-Bliley Act applies to financial services, HIPAA and the HITECH Act apply to protected health information, and FERPA applies to educational institutions and their vendors, along with their implementing regulations, are the most frequently implicated.

Data security and protection requirements at the state level vary significantly, with breach notification laws in all 50 states and some of the more protective privacy regimes existing under the California Consumer Privacy Act, the Virginia Consumer Data Protection Act, the New York SHIELD Act, and the NYDFS cybersecurity regulations.

Finally, US customers with international operations remain subject to international privacy laws like the European Union's General Data Protection Regulation (GDPR).

In addition to the data privacy regulations there is third party risk guidance (from the Federal Reserve, OCC, FINRA, and the NYDFS and other regulatory agencies) that may apply to the use of cloud computing in the financial services industry, and the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) permits federal authorities to compel US-based companies to provide access to data that may be stored on servers in the United States and in other jurisdictions, will also indirectly impact cloud computing, including the offshore storage of data.

In the public sector, the Department of Defence, General Services Administration and NASA jointly issued the Federal Acquisition Regulation (FAR) for use by executive agencies in acquiring goods and services, part 39 of which describes the terms of acquisition of IT, including cloud computing.

The procurement of goods and services by state and local governmental bodies is governed by the procurement laws of the state in question, and, for some municipalities, by applicable municipal codes, some of which may indirectly impact the use and acquisition of cloud computing, especially as the code relates to offshore services.

Breach of laws

11 What are the consequences for breach of the laws directly or indirectly prohibiting, restricting or otherwise governing cloud computing?

There are generally no laws directly applicable to cloud computing. With regard to those laws that may indirectly impact the use of cloud computing, a breach of such laws can result in a variety of consequences. In many cases, violations of these laws result in fines and penalties, and some may subject entities to enforcement actions resulting in consent orders or others settlements. In a few instances, there may be private rights of action related to breaches of these laws.

Consumer protection measures

12 What consumer protection measures apply to cloud computing in your jurisdiction?

There generally are not any consumer laws that are directly applicable to cloud computing. Instead, consumer protection measures are directed at the uses and applications of cloud computing services. For example, in the sales of goods and services to consumers, certain implied warranties will apply and, restrictions on exclusions of liability, jurisdiction requirements and other measures may apply.

The sale of goods and services is typically governed by state law, and different states will apply additional consumer protections. At the federal level, there are a number of laws that offer consumer protection measures, including:

- the Magnuson-Moss Warranty Act;
- the Federal Trade Act;
- the Fair Credit Reporting Act;
- the Gramm-Leach-Bliley Act;
- the Children's Online Privacy Protection Act;
- the Telephone Consumer Protection Act; and
- the Fair Debt Collection Practices Act.

At the federal level, these laws are typically enforced by the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau, but many of these laws also permit private rights of action, enabling consumers to bring direct claims and, in some cases, class actions.

In addition, the data privacy laws and regulations serve as consumer protection measures related to the use and disclosure of personally identifiable information, with enforcement by the FTC at the federal level and by various state entities at the state level.

Sector-specific legislation

13 Describe any sector-specific legislation or regulation that applies to cloud computing transactions in your jurisdiction.

Generally, the laws and regulations that impact cloud computing are sector-specific. For example:

- in the financial services industry, the Gramm-Leach-Bliley Act, third-party risk guidance from the Federal Reserve, OCC, FINRA, and the NYDFS and other regulatory agencies may apply;
- in the higher education industry, FERPA will govern the scope of permitted outsourcing; and
- in the healthcare sector, HIPAA and the HITECH Act along with their implementing regulations will be applicable to the protection of health information.

The type of services also may implicate additional laws.

In addition to sector-specific federal laws related to data protection, data security and protection requirements at the state level may apply and vary significantly. Finally, US customers with international operations remain subject to international privacy laws such as the EU's GDPR.

In the public sector, the DoD, GSA, and NASA jointly issue the Federal Acquisition Regulation (FAR) for use by executive agencies in acquiring goods and services, part 39 of which describes the terms of acquisition of IT, including cloud computing.

The procurement of goods and services by state and local governmental bodies is governed by state procurement laws of the state in question, and, for some municipalities, by applicable municipal codes, some of which may indirectly impact the use and acquisition of cloud computing, especially offshore services.

Insolvency laws

14 | Outline the insolvency laws that apply generally or specifically in relation to cloud computing.

While we are not aware of any US insolvency laws that apply specifically to cloud computing, there are relevant considerations of general US insolvency law in the cloud computing context.

The enforceability of a licence to intellectual property may be impacted by US bankruptcy laws. However, there are provisions in the bankruptcy code (section 365n) that can be leveraged to permit a licensee to continue using the services or other IP in the event of licensor/service provider bankruptcy. The provisions in the service arrangement must be specifically drafted to take advantage of these bankruptcy provisions (including a present grant of a licence to the service or other IP, including any access to source code pursuant to a source code escrow provision).

Termination clauses that permit a party to terminate a cloud contract for the insolvency of the other party may be frustrated by section 365(e) of the US bankruptcy code.

The ability for a customer to retrieve or remove their data from a cloud provider's system may be limited or require leave from the bankruptcy trustee if the cloud provider files for bankruptcy. The reverse would also be true if a cloud provider were to try to remove the data of a customer who had filed for bankruptcy from its systems.

If insolvency of either or both parties is a foreseeable concern, these matters can and should be dealt with proactively in the drafting of the contract.

DATA PROTECTION/PRIVACY LEGISLATION AND REGULATION

Principal applicable legislation

15 | Identify the principal data protection or privacy legislation applicable to cloud computing in your jurisdiction.

There is no uniform federal law governing the processing of personal data in the United States, which is instead governed by a patchwork of federal and state laws.

At the federal level, the most frequently implicated laws (along with their implementing regulations) are:

- the Gramm-Leach-Bliley Act (applicable to financial services);
- the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act (applicable to protected health information);
- the Family Educational Rights and Privacy Act (applicable to educational institutions and their vendors); and
- the Children's Online Privacy Protection Act (governing collection of personal information from children online).

Data security and protection requirements at the state level vary significantly, with breach notification laws in all 50 states and some of the more restrictive privacy regimes existing under the California Consumer Privacy Act and the California Privacy Rights Act (which is being phased in and coming fully online on 1 July 2023), the Virginia Consumer Data Protection Act, the Colorado Data Privacy Act (coming online on July 1, 2023), the New York SHIELD Act, and the New York State Department of Financial Services' cybersecurity regulations.

Finally, US customers with international operations remain subject to international privacy laws like the European Union's General Data Protection Regulation (GDPR) and the UK's implementation of the GDPR in the Data Protection Act 2018.

The features of and requirements under these laws vary greatly and, depending upon the law(s) implicated by the services arrangement may include:

- both general and specific data security requirements;
- notices and disclosures to data subjects regarding data collection, usage and transfers;
- rights of access, correction, deletion, portability and opt-out;
- data minimisation;
- data protection assessments;
- federal and state enforcement (including the right to impose fines and penalties); and
- private rights of action.

CLOUD COMPUTING CONTRACTS

Types of contract

16 | What forms of cloud computing contract are usually adopted in your jurisdiction, including cloud provider supply chains (if applicable)?

Cloud computing contracts in the United States typically are on the cloud service provider's paper and are comprised of a master service agreement (usually a cloud services agreement, master subscription agreement, or master software as a service agreement) setting out general terms and conditions that govern one or more order forms or ordering documents entered into by the parties that specifically list the services being acquired, any service-specific terms, pricing, payment and other relevant business terms.

Cloud contracts are highly modular and, given the evolutionary nature of cloud services and the right of the provider to modify services to meet market demand, often include and incorporate by reference to myriad online terms via an URL. These online terms usually describe the services, service levels, data processing and data security terms, business continuity and disaster recovery capabilities, any applicable third-party service terms or flow downs and other more detailed terms related to the services. While most cloud providers take the position that the online terms are non-negotiable because the terms are operational in nature, customers with sufficient negotiation leverage often have success in negotiating these terms to address key requirements.

In a negotiated transaction, it is often the case that the online terms may conflict with the negotiated terms of the master agreement and the order forms. Cloud services customers will seek to have the negotiated terms govern in the event of a conflict, and savvy customers will seek to have the online terms included in the contract or identified by date or version number to set a baseline for the governing terms as of the effective date of the cloud services contract, both generally and for purposes of any warranty against material adverse changes to the services or the governing terms.

If professional services are required for implementation, deployment, configuration, or training, those professional services are usually governed by a separate professional services agreement, so that issues

related to the professional services do not jeopardise the subscription and subscription revenues. With that said, some providers will enter into professional services statements of work or orders under the same master agreement as governs the cloud services subscription, albeit still with separation of remedies for professional services work from any remedies that might permit cancellation or termination of the subscription.

Typical terms for governing law

17 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering governing law, jurisdiction, enforceability and cross-border issues, and dispute resolution?

Most US contracts, including cloud computing contracts, will specify the state the governing law of which will govern the terms and interpretation of the contract, and it is customary for the parties to choose a forum within the same state for resolution of disputes. Typically, the state where the cloud service provider is located is selected by the provider as its preferred governing law. However, many customers will seek to impose the governing law of a neutral jurisdiction with more broadly known and understood common law outcomes (eg, New York or Delaware). The parties must be careful to ensure that there is some reasonable nexus between the arrangement and the selected state whose law governs in order for the governing law election to be upheld. With that said, New York and Delaware governing law selection will generally be upheld if the value of the contract meets applicable thresholds (currently, $250,000 in New York and $100,000 in Delaware). When drafting a governing law clause, it is customary to disclaim the applicability of the selected state's principles regarding conflicts of laws, as those principles may subvert the selection made by the parties. Similarly, many contracts will disclaim the applicability of the Uniform Computer Information Transactions Act and the United Nations Convention on Contracts if, and as applicable, as each could also subvert the desired predictability of the selected governing law.

Most cloud computing contracts resort to either litigation or binding arbitration for dispute resolution, although sometimes mediation is a precursor to litigation. While common in other services arrangements, cloud computing contracts less often include informal dispute resolution as a precursor to formal dispute resolution. In all cases, the contracts will often specify the federal and/or state courts for the resolution of litigated disputes, taking into account facts relevant to personal jurisdiction requirements under federal and state law. US customers with foreign-domiciled providers often prefer arbitration, with the preferred arbitral rules and tribunal varying based upon where the parties are domiciled and other factors. If arbitration is chosen, the parties will usually reserve certain matters for litigation (eg, equitable relief, confidentiality, intellectual property).

Typical terms of service

18 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering material terms, such as commercial terms of service and acceptable use, and variation?

Pricing and payment

Pricing for cloud services is usually expressed as a subscription fee and may be tied to myriad variables that drive utilisation of the cloud service and vary greatly depending upon whether the services is infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS) or other forms of anything-as-a-service (XaaS). The definitions of those variables often require and receive close scrutiny and negotiation in order to align the drivers of cost with the intended usage of the service.

In some shape or fashion, the subscription fees usually result in a minimum, non-cancellable spend commitment from the customer, whether that takes the form of a minimum commitment, a volume discount, or a set subscription fee for defined services. It is common for subscription fees to be billed in advance, either annually, quarterly or monthly, and sometimes for the full term in advance. Customers will often negotiate pricing for renewal terms, with any inflationary adjustments being both indexed to an inflationary index and also subject to a cap, as well as pricing for additional quantities of services that extend to future purchases (including where true-up is required due to overutilisation).

Pricing for one-time professional services (eg, installation, implementation, configuration, training etc) may be governed by separate professional services agreements, or under the same agreement that governs the cloud services. In either case, training is usually invoiced with the subscription, and other professional services may be invoiced on a time and materials basis (usually monthly in arrears) or on a fixed-fee basis (often tied in whole or in part to acceptance of defined milestones).

Default payment terms on provider paper are most often net 30 from the date of the invoice, although customers will negotiate for longer payment terms (60-90 days) from receipt (as opposed to the date) of the invoice. Whether or not customers have the right to withhold disputed amounts, the period within which disputes must be identified and whether or not interest is payable on late payments are all negotiable items and vary depending upon the complexity of the fee structure and the likelihood of billing errors and disputes. If the customer fails to pay undisputed amounts when due, the service provider has the right to terminate the services and often also has the right to suspend services prior to electing to terminate.

Acceptable use policies

Most cloud services contracts will require the customer and their authorised users to comply with the service provider's acceptable use policy (AUP), which usually prohibits some or all of the following:

- usage by third parties (other than authorised users);
- usage as a service bureau or to provide services to third parties;
- reverse engineering, decompiling or otherwise trying to discover the source code of the services;
- modifying or creating derivative works of the service;
- illegal activities of any kind or posting illegal, offensive or libellous or defamatory content;
- violation of any third-party rights;
- gaining or attempting to gain unauthorised access to any networks, systems, devices or data, including conducting penetration testing;
- unauthorised disruption of any networks, systems, devices or data;
- sending unsolicited messages or marketing; and
- distributing or uploading malware to the service.

It is common for the service provider to have the right to suspend service (and in some cases, terminate the contract) if the customer or its authorised users violate its AUP. Customers will negotiate for notice and the opportunity to cure, which is often granted where practical in view of the impact of the violation in question, and most providers will agree to promptly restore service after the violation is cured.

Variation

Because many cloud services offerings are mass market, multitenant offers, most providers will reserve the right to unilaterally modify the cloud services, presumably to improve the service to meet the demands of the mass market. Whether notice is required and what recourse the customer has in connection with those modifications are often negotiated. Most negotiated agreements will provide:

- that the service provider will provide notice of any changes to the service in accordance with its standard service delivery policies (usually via a customer portal);
- that the changes will not have a material and adverse impact on the service (sometimes this restriction extends also to the terms of service and the features, functionality and security of the service); and
- that the service provider must remediate any material adverse change within a defined period (usually 30 days), failing which the customer will have the right to terminate the services (and often the entire agreement) and receive a refund of any prepaid fees for periods following the effective date of termination.

Typical terms covering data protection

19 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering data and confidentiality considerations?

Confidentiality

Cloud computing contracts will almost often include a mutual confidentiality provision providing that each party's confidential information is proprietary and restricting each party's disclosure of, and requiring each part to use reasonable measures to protect, the other party's confidential information. Disclosures to employees, contractors, attorneys and accountants and sometimes third parties are usually permitted as required to fulfil obligations and exercise rights under the contract, with the receiving party being required to impose equally protective confidentiality terms on downstream recipients and being primarily liable to the disclosing party for the acts and omissions of those recipients.

The definition of confidential information will almost always include the cloud service and will usually require some modification to accommodate customer confidential information. These confidentiality provisions will almost always carve out customer data, which is subject to separate provisions as discussed in more detail immediately below.

Data integrity

The default provider position is that the customer is responsible for the accuracy and quality of its data. Of course, such a general statement does not satisfy many customers' requirements, and the parties will often agree to bifurcate responsibility such that the customer has responsibility up to the point it is provided to the provider for processing (and for any changes made by the customer), and the provider assumes responsibility at the point the data is provided for processing. Even under that bifurcated structure, the provider will often limit its liability for restoring data to restoring to the latest backup. In addition, cloud computing contracts usually provide that the customer owns its data, with customers often negotiating to include the results of processing of their data within the realm of ownership.

Data preservation

The architecture of the cloud service will dictate which party is responsible for backing up the customer's data, with the norm being that data storage and backup is a part of the cloud service, with the service provider being responsible for backups. The frequency of those backups and the resultant recovery point objectives are usually viewed as a feature of the service, with some providers having varying levels of service at different price points. The terms governing backup and recovery are often the subject of a service provider policy or services documentation that is incorporated into the contract by reference to an URL.

Systems, premises and data security

Terms covering systems, premises and data security usually take the form of:

- a data processing addendum or agreement that obligates the service provider to implement technical and organisational security measures as required to comply with the standards required by applicable privacy laws;
- provider disaster recovery and security policies or services documentation that are incorporated into the contract by an URL; and
- third-party certifications (eg, SOC 2 Type 2, ISO 27001, HITRUST, PCI, etc).

The nature and scope of these terms will vary from provider to provider and also from service to service with a single provider. For example, some providers have designated (higher cost and more secure) environments for processing certain types of data (eg, payment card data) or where the customer requires a more secure or a higher-availability environment. Customers will often require the service provider to complete an information security questionnaire, which the customer will then need to compare with the service provider's security and disaster recovery commitments in the cloud computing contract.

Data usage, disclosure and retention

Usage, disclosure and retention of customer data by the service provider are often limited to only that which is required to provide the service, although exceptions for retention and disclosure required by law and usage of aggregated and/or de-identified data for service improvement and other purposes are becoming more commonplace in today's big data world.

Exceptions for retention in accordance with industry-standard backup and retention policies are also fairly common, with the data protection terms of the contract continuing to apply during the period of retention. All of these exceptions are often carefully negotiated to avoid triggering unintended or adverse consequences under applicable privacy laws (eg, a resale under the California Consumer Privacy Act).

Location of servers and data

Customers often seek to limit access to and storage of their data to defined jurisdictions, in which case, those limitations must be specified in the contract (usually in the order form or ordering document or in the provider policies or services documentation incorporated into the contract). There may be separate provisions governing where data is stored versus where data may be accessed, especially where the provider leverages support resources in different geographies to provide follow-the-sun support.

Cross-border data transfers

There are no geographic transfer restrictions on personal data generally in the United States. However, there are some limitations on the transfer of certain data in the custody of certain federal and state agencies (eg, federal income tax data). However, many US customers have international operations in jurisdictions that do impose more onerous requirements on cross-border data transfers (eg, in the United Kingdom and the European Union). In most cases, cross-border data transfers will be dealt with in a data processing addendum or agreement that forms part of a cloud computing contract, with the terms being consistent with the cross-border data transfer requirements of the more onerous of the global data privacy regimes (at the moment, the General Data Protection Regulation (GDPR) and its progeny pursuant to the European Court of Justice's ruling in *Schrems II*).

Typical terms covering liability

20 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering liability, warranties and provision of service?

The cloud deployment model has created a fairly standardized (provider-friendly) contracting framework in the United States. The issues that are most negotiated include many of those covered by this question.

Provider warranties and customer remedies

Most cloud computing contracts will include a warranty that the service will perform materially or substantially in accordance with the specifications or documentation, and a warranty that changes to the cloud services will not have a material and adverse impact on the service (sometimes this restriction extends also to the terms of service and the features, functionality and security of the service). Often (especially in negotiated contracts), the contract will require that the service provider remediate any breach of either of those warranties within a defined period (usually 30 days), failing which the customer will have the right to terminate the services (and often the entire agreement) and receive a refund of any prepaid fees for periods following the effective date of termination. These remedies are often the customer's sole and exclusive remedies for a breach of the foregoing warranties, although care should be taken to avoid any conflict between the sole and exclusive remedy warranty remedy and any service level credits or other remedies (as described below).

If the cloud computing contract also covers professional services, it would also be common for the provider to warrant that the services will be performed in a professional and workmanlike manner in accordance with industry standards, that the deliverables will conform to the applicable specifications and/or acceptance criteria, and that any documentation of the deliverables will be sufficient to enable a reasonably qualified IT professional to support, maintain and make use of the deliverables. If the provider breaches these warranties, the remedies usually include no-cost correction or re-performance, and often a refund if the provider is unable to correct or re-perform. The amount of the refund is negotiable, with the provider taking the position the refund is limited to amounts paid for the deficient services or deliverables, while customers often negotiate for a refund of fees paid under the applicable statement of work or the agreement, and the right to terminate the same.

Non-infringement warranties are extremely uncommon for subscription services, but they are more common for related professional services, where the customer would suffer out-of-pocket costs to correct infringing deliverables above and beyond amounts payable to the third-party claimant for the infringement.

Customer warranties

Customer warranties are less common in the cloud computing context, although providers will sometimes require that the customer represent and warrant that the customer has the requisite consents to permit the provider to process the customer data as contemplated by the agreement.

Warranty disclaimer

Providers will often include broadly worded disclaimers in cloud computing contracts providing that the warranties in the agreement are the sole and exclusive warranties and disclaiming all other warranties, including implied warranties of non-infringement, merchantability, and fitness for a particular purpose. Sometimes these disclaimers provide that the services are provided as-is. Customers frequently revise these disclaimers to avoid any inconsistency with other commitments made in the agreement, including within provider warranties and the service levels.

Service availability, reliability and quality

Most cloud computing contracts include or incorporate by reference to an URL leading to the provider's standard service level commitments and other service descriptions, and support policies that will define the availability, reliability and quality of the services. The service levels almost always include availability and incident response time, although sometimes incident response is dealt with in a separate support policy. For SaaS services, the service levels may also include commitments related to the performance of certain attributes of the software. Credits for service level failure are common but are usually limited to a subset of the service levels offered.

Providers will take the position that these terms are not negotiable, but customers with sufficient negotiation leverage often have success in negotiating custom service levels. The most commonly negotiated improvements are:

- heightened availability commitments;
- incident resolution commitments (in addition to incident response);
- increased credits for service level failures; and
- a right to terminate for repeated or significant service level failures.

Many providers take the position that service level credits are only applied if the customer raises a ticket for the applicable service level failure, although customers often negotiate a more proactive reporting and credit application process.

Business continuity and disaster recovery

Business continuity and disaster recovery commitments made by cloud computing providers are usually viewed as a feature or attribute of the service, with some providers having varying levels of service at different price points. The terms governing business continuity and disaster recovery are often the subject of a service provider policy or services documentation that is incorporated into the contract by reference to an URL. For critical infrastructure and applications, customers will pay close attention to these policies and documentation and will often negotiate to include defined recovery time objectives (setting the minimum period for recovery from a disaster) and recovery point objectives (setting the minimum currency of data restored from backup), if those commitments are not already set forth in the applicable policy or documentation.

Limitation of liability

Most cloud computing contracts, because they are almost always on provider paper, will include a provider-friendly limitation of liability provision that:

- limits the provider's liability under the agreement to a monetary cap, which is usually specified in terms of the fees paid by the customer for the affected service for some number of months (usually 12 months, although some providers start as low as three months) prior to the claim; and
- disclaims indirect, special, consequential and punitive damages, and often lost profits, reputational harm, diminution in value, data loss, costs of cover or replacement services and similar damages.

Customers often negotiate improvements to the standard provider liability framework, which customarily include:

- making the limitations mutual, if not already; and
- carving out from those limitations:
  - the parties' indemnification obligations; and
  - liability for breaches of the data privacy and security provisions of the agreement, although these damages are often subject to separate limitations on the amount recoverable (usually two times the general cap, but sometimes expressed as a much higher amount in high-risk/low-spend situations),

and on the types of damages recoverable (usually limited to some or all of:
  - the cost of providing notice to affected data subjects;
  - credit monitoring and fraud insurance for affected data subjects;
  - the cost of operating a call centre and website to communicate with affected data subjects;
  - the cost of investigation and remediation;
  - attorneys' and consultants' fees; and
  - fines, penalties and interest); and
- damages resulting from a party's gross negligence, wilful misconduct or fraud;
- sometimes, damages resulting from a party's breach of applicable law;
- fees payable by the customer; and
- the customer's breach of the licence or intellectual property terms of the contract.

Indemnification

Most cloud computing contracts will include an indemnity from the provider in favour of the customer covering third-party claims that the cloud services infringe the intellectual property rights of the third-party claimant. Sometimes, the scope of the indemnity will be limited to US patents, copyrights and trademarks, although customers will resist those limitations. The indemnity will usually exclude claims arising from the use of the services in breach of the contract, combinations of the services with other software or technology, modifications to the services not made by the provider, and the customer's requirements and data. Customers will seek to make those exclusions comparative (ie, applicable only 'to the extent' the claim is caused by the exclusion) and to exempt from the exclusion use as contemplated by the contract or the applicable specifications or documentation.

Other indemnities

Other indemnities may include:

- a reciprocal infringement indemnity from the customer covering materials and data furnished by the customer;
- an indemnity in favour of the customer for breach of the data privacy and security provisions of the contract;
- a mutual indemnity for breaches of applicable law (less common); and
- an indemnity in favour of provider for customer's use of the service (although care should be taken in this instance to avoid overlap and conflict with claims that are subject to indemnification by the provider).

In all cases, these indemnities would be limited to third-party claims and subject to the limitations of liability and applicable exclusions described above.

Typical terms covering IP rights

21 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering intellectual property rights (IPR) ownership in content and the consequences of infringement of third-party rights?

Intellectual property rights ownership

In most, if not all, cases, the provider will own all rights, titles and interests in and to the cloud computing services and the intellectual property rights therein. The same will usually be true for improvements and modifications made to the cloud computing services, although there are exceptional circumstances where the customer may seek to own, or have an exclusive licence for a period to, improvements and enhancements that are highly proprietary to the customer or funded at customer's expense.

The customer typically owns the customer data and all derivations thereof, with the exception of aggregated and de-identified data, which providers will sometimes seek to carve out from the scope of customer data ownership. The contract may also specify customer's ownership of its pre-existing intellectual property.

Infringement

Infringement is most often addressed via indemnification – by the provider for infringement claims related to the cloud computing services and by the customer for infringement claims related to the customer data or other intellectual property furnished by the customer. Non-infringement warranties are almost always disclaimed with regard to cloud computing services but may be negotiated for related professional services.

Typical terms covering termination

22 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering termination?

Termination rights

Most cloud computing contracts will include a mutual right for each party to terminate the other party's material breach that remains uncured for more than 30 days following receipt of notice of the breach. The contract may also separately permit termination by the customer for cause for the provider's uncured breach of the service performance warranty or the warranty against material adverse changes to the services, as well as for defined repeated service level failures. In rarer cases, the contract may permit the customer to terminate for a breach of the privacy and security provisions of the contract that results in a compromise of customer data.

Termination for convenience is less common in cloud computing contracts, as most cloud subscriptions are non-cancellable. However, some providers reserve the right to terminate the service for convenience if they cease offering the services generally.

Transition and data migration

The default position in most provider contracts is that the provider will, for a period (usually 30-90 days) following expiration or termination of the contract, make the customer's data available for download by the customer. Such a limited commitment is often insufficient for customers buying more critical services that might take more time to transition. Accordingly, most customers will negotiate for a period of continued usage of the cloud services (anywhere from 90 days to 24 months depending upon complexity) during which the customer can migrate to a replacement solution. If agreed, any additional provider cooperation required during that period to effect the migration will be separately charged. Finally, savvy customers will negotiate more specificity around the format in which the customer data will be made available upon exist, usually specifying a defined format (eg, CSV) or more generally referring to a format that is usable with generally commercially available off-the-shelf productivity software.

The provider may be permitted to retain customer data beyond expiration or termination of the contract if required by law or in accordance with an industry-standard backup policy, in all cases subject to the data privacy and security terms of the contract.

Employment law considerations

23 Identify any labour and employment law considerations that apply specifically to cloud computing in your jurisdiction.

There are no US employment law considerations specifically applicable to cloud computing. To avoid any risk of co-employment, most US cloud computing contracts (and most US services contracts generally) will include a provision that provides that the parties are independent contractors and that the agreement does not create any agency, partnership, joint venture, or another form of joint enterprise, employment or fiduciary relationship between the parties.

TAXATION

Applicable tax rules

24 Outline the taxation rules that apply to the establishment and operation of cloud computing companies in your jurisdiction.

In general, taxes in the United States apply to what you earn, what you buy and what you own. For corporate entities, these taxes are imposed at the federal and state level and may include corporate income taxes, payroll taxes, capital gains taxes, sales and use taxes, gross receipt and margin taxes, excise taxes, property taxes and tangible personal property taxes. In addition, depending on the use and application of cloud computing services, additional taxes may apply.

Some of the most rapidly changing aspects of the tax environment in the United States relate to cloud computing and the taxation of digital goods and services sold or delivered remotely. Many state and local tax authorities have expanded, and others are expanding, their income and sales tax rules to include digital goods and services. Each of these states' and localities' rules differ and will apply to cloud computing differently depending on the implementation, delivery model and application of each (eg, software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS)). In addition, there are apportionment rules that apply on a state and locality basis related to the physical and economic nexus of the company and the business and consumer to which it is selling the goods and services.

Also of importance, as a result of the pandemic, the tax landscape relative to remote workers, often accessing corporate networks via cloud computing, is increasingly complex with states vying for their share of the revenue. For example, the presence of remote workers in new states may create nexus and subject the company to new state taxes.

Indirect taxes

25 Outline the indirect taxes imposed in your jurisdiction that apply to the provision from within, or importing of cloud computing services from outside, your jurisdiction.

In general, taxes in the United States apply to what you earn, what you buy and what you own. For corporate entities, these taxes are imposed at the federal and state level and may include corporate income taxes, payroll taxes, capital gains taxes, sales and use taxes, gross receipt and margin taxes, excise taxes, property taxes and tangible personal property taxes. In addition, depending on the use and application of cloud computing services, additional taxes may apply.

Some of the most rapidly changing aspects of the tax environment in the United States relate to cloud computing and the taxation of digital goods and services sold or delivered remotely. Many state and local tax authorities have expanded, and others are expanding, their income and sales tax rules to include digital goods and services. Each of these states' and localities' rules differ and will apply to cloud computing differently depending on the implementation, delivery model and application of each (eg, SaaS, IaaS, PaaS). In addition, there are apportionment rules that apply on a state and locality basis related to the physical and economic nexus of the company and the business and consumer to which it is selling the goods and services.

Also of importance, as a result of the pandemic, the tax landscape relative to remote workers, often accessing corporate networks via cloud computing, is increasingly complex with states vying for their share of the revenue. For example, the presence of remote workers in new states may create nexus and subject the company to new state taxes.

RECENT CASES

Notable cases

26 Identify and give details of any notable cases, or commercial, private, administrative or regulatory determinations within the past three years in your jurisdiction that have directly involved cloud computing as a business model.

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) enacted on 23 March 2018 indirectly impacts cloud computing, including the offshore storage of data. The Act permits federal authorities to compel US-based companies to provide access to data that may be stored on servers in the United States and in other jurisdictions. Part of the motivation for the CLOUD Act related to *United States vs Microsoft Corp*, 138 S. Ct. 1186 (2018), in which Microsoft objected to providing the content of an account holder's emails that was stored in Ireland. The CLOUD Act enabled the United States to gain access to the contents.

The Supreme Court's decision in *South Dakota v Wayfair* 585 U.S. ___; 138 S. Ct. 2080; 201 L. Ed. 2d 403 was a landmark decision for nearly all businesses delivering digital goods and services, many via the use of cloud computing. The application of the economic nexus for sales tax determination expanded businesses' obligations to collect and remit sales tax in new states, where previously such tax obligations related more on a physical nexus. The *Wayfair* decision continues to have a significant ripple effect on the cloud industry.

There are also a variety of other states that are attempting to expand the collection of revenue, including Maryland which has implemented a new digital advertising tax. This tax is currently suspended pending administrative and legal challenges. This and other similar new legislation and legal challenges will be important to follow.

Finally, last October, the US House Judiciary Committee included cloud computing in its report Investigation of Competition in Digital Markets which looks at issues of conflict and the impact of dominant incumbent platforms affecting innovation and market entry of new businesses. Market leaders in the cloud benefitted from early-mover advantage, coupled with network effects and high switching costs that can lock in customers. The report also highlighted specific techniques used to deter switching by customers, such as long-term contracts, free tier products (which tend to deter switching to a new provider at the end of a free trial period, due to the investment of time and resources required to adapt to a new provider as well as the requirement to pay exit fees to the original provider). Exit fees can create significant financial barriers to migration away from specific providers, coupled with technical design challenges to adapt to the new cloud service provider's method of operating its services. Portability, exit costs and interoperability are therefore likely to be at the forefront of regulatory concern. Market participants are monitoring for further action coming out of this report.

UPDATE AND TRENDS

Key developments of the past year

27 What are the main challenges facing cloud computing within, from or to your jurisdiction? Are there any draft laws or legislative initiatives specific to cloud computing that are being developed or are contemplated?

The main challenges facing cloud computing in the United States largely track those facing the industry globally and include mitigating continued and evolving threats to information and data security, an uptick in ransomware activity, the ability to hire and retain qualified human resources, and supply chain shortages and disruptions.

Legislatively speaking, there are, at present, six bills wending their way through Congress that would impact the cloud computing market generally, and Microsoft, Google and Amazon specifically. In the main, these legislative bills seek to curtail the market power of Big Tech by splitting these companies up, targeting their ownership of online platforms in combination with other lines of business, or establishing a framework for data portability and interoperability. Since these bills have received some bipartisan support, we think it is very likely that the United States will enact some form of federal legislation impacting Big Tech and the principal cloud services providers in the near future.

Further, market participants also continue to monitor for additional action on the recommendations coming out of the US House Judiciary Committee's Investigation of Competition in Digital Markets report which looked at issues of conflict and the impact of dominant incumbent platforms affecting innovation and market entry of new businesses.

BRYAN CAVE LEIGHTON PAISNER BCLP

Sean Christy
sean.christy@bclplaw.com

Chuck Hollis
chuck.hollis@bclplaw.com

Derek Johnston
derek.johnston@bclplaw.com

One Atlantic Center
14th Floor
1201 W Peachtree Street NW
Atlanta
Georgia
30309-3471
United States
Tel: +1 404 572 6600
Fax: +1 404 572 6999
www.bclplaw.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-634-1