CHAPTER 2

Dear Cloud, I Think We Have Trust Issues: Cloud Computing Contracts and Trust

Theo Lynn

Abstract Cloud computing is the dominant paradigm in modern computing, used by billions of Internet users worldwide. It is a market dominated by a small number of hyperscale cloud service providers. The overwhelming majority of cloud customers agree to standard form clickwrap contracts, with no opportunity to negotiate specific terms and conditions. Few cloud customers read the contracts that they agree to. It is clear that contracts in cloud computing are primarily an instrument of control benefiting one side, the cloud service provider. This chapter provides an introduction to the relationship between psychological trust, contracts and contract law. It also offers an overview of the key contract law issues that arise in cloud computing and introduces some emerging paradigms in cloud computing and contracts.

Keywords Contract law • Terms of service • Cloud computing • Cloud contracts • Trust

T. Lynn (✉)
Irish Institute of Digital Business, DCU Business School, Dublin, Ireland
e-mail: theo.lynn@dcu.ie

T. Lynn et al. (eds.), *Data Privacy and Trust in Cloud Computing*,
Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-030-54660-1_2

2.1 Introduction

Since the 1990s, outsourcing information systems has been a staple of business strategists. They argue that firms should focus on their core competencies and outsource all other activities to optimise resource allocation (Lambert and Peppard 2013). The emergence of what the International Data Corporation (IDC 2013) term the 'Third IT Platform' comprising cloud computing, social media, mobile and big data/analytics technologies has accelerated the outsourcing of critical information systems.

Cloud computing has emerged as the dominant computing paradigm of the twenty-first century. It is defined as a "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance 2011, p. 2). Enterprise cloud IT expenditure consistently exceeds non-cloud expenditure for enterprises of all sizes (IDC 2020). Despite the ubiquity of cloud computing, a small number of hyperscale cloud service providers (CSPs) dominate the public cloud market. In 2018, five companies accounted for nearly 77% of the global Infrastructure-as-a-Service (IaaS) market—Amazon, Alibaba, Google, IBM, and Microsoft (Gartner 2019). As cloud computing is the basis of the Internet, including most social networking sites, search engines, and mobile applications, over 3.6 billion Internet users rely on cloud computing for one or more services. For firms, the benefits of increased IT efficiencies, agility, and scalability (both up and down) must be weighed against the risks that these technologies pose to firm performance, relationships, and compliance (Lynn and Rosati 2017). Similarly, for individuals, they must weigh up the utility of the functionality they receive from the applications that they subscribe to, and the risk to their data privacy.

For the most part, cloud computing contracts are standard form and click-wrap in nature, with only the largest corporate and government customers in a position to negotiate tailored terms and conditions (Bradshaw et al. 2013). As part of this click-wrap procedure and before payment, prospective clients are typically presented with either (1) a scrollable agreement, or (2) a link to a webpage or downloadable agreement, based on the specific cloud service and configuration that they have selected. They are encouraged to review the text of the agreement, and asked to communicate assent to the terms and conditions by clicking on an interactive 'I agree' button. For the overwhelming majority of CSP clients, these

click-wrap contracts are standardised wholly electronic contracts giving the clients little or no opportunity to negotiate specific terms and conditions. As such, the vast majority of cloud customers need to balance the tension of the advantages of the cloud against the disadvantages of boilerplate terms and conditions designed by global firms with legal resources several orders of magnitude greater than even the largest law firms, as well as the perceived and actual loss of control. In the absence of alternatives, cloud customers may feel that they have no choice but to rely on these contracts to eliminate distrust or mitigate the negative impact of a trust violation, in effect a form of what Lewicki et al. (2006) refer to as calculative trust. Similarly, they may simply agree to the terms and conditions as an anxiety avoidance mechanism (Weber et al. 2004; van der Werff et al. 2019). Either way, a trust issue arises.

This chapter provides an overview of common terms and conditions in general form cloud computing click-wrap contracts. To avoid repetition, we assume the general definitions of trust and cloud computing presented in Chap. 1. The remainder of the chapter is organised as follows. Following a brief discussion on the theoretical relationship between trust, contracts and contract law, the structure of cloud computing contracts is introduced. This is followed by an overview and discussion of the key terms and conditions in cloud computing contracts and the issues that these present. Then, we discuss briefly how the nature of cloud computing and contracts are evolving before concluding with a brief discussion of the trust implications resulting from these issues.

2.2 Trust, Contracts and Contract Law

Trust and distrust are inextricably linked to the moral and legal underpinnings of Anglo-American contract law. The purpose of this chapter is not to justify trust as a theoretical building block of contract law but rather outline contractual issues in cloud computing and how these might impact trust in cloud computing and CSPs. However, understanding the relationship between trust, contracts and contract law, even at a high level, may provide insights in to the role of cloud computing contracts play in the relationship between CSPs and their clients. At the core of a contract is a promise where "a person invites another to trust, and to break a promise is to abuse that trust" (Bellia Jr 2002, p. 25). But, what is the nature of this trust? And what is the relationship between trust, contracts, and contract law?

As discussed in Chap. 1, psychologists suggest that when we trust someone, we accept vulnerability based on positive expectations of the future behaviour of that party (Rousseau et al. 1998). Inherent in this trust, is the assumption that the other party (1) possesses the necessary skills and capabilities to deliver on the promise (ability); (2) has the trustor's interests at heart (benevolence); and (3) will adhere to a set of mutually acceptable principles for behaviour (integrity) (Mayer et al. 1995).

Kimel (2001) suggests that while promises draw on the same reliance and expectation of fulfilment that exists in personal trust, contracts are different than promises and exist outside of the framework of personal relationships. He argues that contracts, in fact, undermine the concept of psychological trust and human relationships and, in effect, exist as a substitute to trust (Kimel 2001). In contrast, Bellia Jr (2002) argues that the intrinsic value of a promise, regardless of enforceability, does not lie in its capacity to reinforce trust relationships but rather in the knowledge that certain promises need to be enforced. Similarly, Lumineau (2017) posits that a lack of trust does not necessarily signify distrust, and indeed argues that both trust and distrust can result in positive and negative outcomes.

Legal theorists use similar constructs to argue why the law should enforce a contract. Trust is conceptualised in a number of different ways in contract law theory. For example, autonomy theory argues that the enforcement threat in contract law exists to enhance the freedom of the promisor and respects the trust of the promise, while welfare-economic theorists argue it exists to maximise individual or social well-being (Bellia Jr 2002). In reality, contract law exists to perform a variety of trust-related functions including enabling parties to make and enforce a promise, avoid conflicts, and regulate coordination and cooperation between them (Bellia Jr 2002).

2.3 The Form of General Cloud Computing Contracts

The contractual relationship between CSPs, their clients, and crucially their clients' end users, are typically set out in a standard form click-wrap contract comprising the following four components:

- Terms of Service (TOS)—the TOS set out the provisions that define and regulate the overall relationship between a CSP and the client.

- Service Level Agreement (SLA)—the SLA details the level of service to be provided, often in the form of specific quality of service (QoS) metrics, and the mechanisms for auditing service delivery and QoS, and compensating clients for underperformance.
- Acceptable Use Policy (AUP)—sometimes called a 'fair use policy', the AUP is a policy to protect CSPs from the actions of clients, and in the case of enterprise clients, their end users, by detailing prohibited uses of the contracted cloud service.
- Privacy Policy—this details the CSP's policy for handling and protecting personal data, in line with data protection law requirements.

Click-wrap contracts are part of a common cloud service subscription procedure made over the Internet. As part of this procedure and before payment, prospective clients are typically presented with either (1) a scrollable agreement, or (2) a link to a webpage or downloadable agreement, based on the specific cloud service and configuration that they have selected. They are encouraged to review the text of the agreement, and asked to communicate assent to the terms and conditions by clicking on an interactive 'I agree' button. For the overwhelming majority of CSP clients, these click-wrap contracts are standardised wholly electronic contracts giving the clients little or no opportunity to negotiate specific terms and conditions. Bradshaw et al. (2013) notes three distinctions within cloud computing contracts—(1) free vs paid services, (2) US v EU jurisdictions, and (3) IaaS v Software-as-a-Service (SaaS). First, they note that some terms and conditions for paid services are more likely to be open to negotiation depending on the bargaining power of the prospective client e.g. large multinational corporations or Governments. In these cases, depending on the standing of the CSP in the market or the specific segment, there may be a relationship of interdependence rather than dependence (McKnight et al. 2002). This is particularly evident cloud application and API marketplaces (Paulsson et al. 2020). Second, contracts offered under US law have more extensive disclaimers of warranty and limitations of liability than those offered under European Union (EU) law (Bradshaw et al. 2013). Thirdly, terms and conditions offered by IaaS providers would seem to be more similar than those offered by SaaS providers (Bradshaw et al. 2013).

In contract law, the so-called 'informed minority' hypothesis has been used to justify the avoidance of regulation of standard form contracts (Bakos et al. 2014). This hypothesis posits that there is generally a

significant number of informed consumers in any given market to make an informed decision on the terms of a standard-form contract, and that while a substantial number, if not the majority, of consumers may remain uninformed, the former is of significant size to discipline abuse by the market (Schwartz and Wilde 1978). Extant research has found that Internet users consistently do not read such click-wrap contracts. For example, Bakos et al. (2014) found only 0.2% shoppers access a product's end-user license agreement for at least one second. As mentioned earlier, this may be due to a combination of dependency and anxiety avoidance on behalf of the cloud consumer (Weber et al. 2004; van der Werff et al. 2019). To counter this, policymakers have sought to mandate both disclosure of terms and conditions, and acceptance (van der Wees et al. 2014). Notwithstanding this, research suggests accessibility and mandatory acceptance do not result in significant increases in reading click-wrap contracts, and even those who have read the contracts, do not change their decision or behaviour (Marotta-Wurgler 2012). While there is a paucity of similar research on firm behaviour with regards to click-wrap contracts, it is likely to be similar, particularly for smaller organisations. The reality is accepting click-wrap contracts has become a habitual and an inevitable part of cloud computing. By not reading the terms and conditions of these click-wrap agreements, there is no incentive for CSPs to provide anything more than the minimum legal requirements. As such, most cloud contracts are extremely one-sided (Bradshaw et al. 2013) and would not seem to be subject to the informed minority rule (Schwartz and Wilde 1978).

The enforceability of electronic click-wrap agreements has been upheld by courts worldwide for both business-to-consumer and business-to-business transactions, and for paid and free services, tending towards supporting the position of the service provider (see for example, *Rudder v Microsoft Corp*, *Caspi v Microsoft Network*, and *El Majdoub v CarsOnTheWeb. Deutschland GmbH*). The main arguments are both freedom of contract arguments i.e. that clients have the opportunity to make themselves familiar with the terms and conditions and that they provide consent, and economic arguments i.e. rendering click-wrap contracts ineffectual, even though one-sided, would disrupt e-commerce and not be in the public interest.

2.4 Common Challenges and Issues in General Cloud Computing Contracts

2.4.1 Choice of Law

By definition, cloud computing is a distributed model. Data can be, and most likely will be, stored and processed across multiple data centres, potentially in different jurisdictions, and even where stored and processed in one jurisdiction, may be transferred across borders and accessed in different jurisdictions. It is possible that the provider and the end user are unaware of where the data is processed. For enterprise clients, the TOS increasingly allow data residency in a specific region; a region may be a country or a larger area such as the European Union. While consumer cloud users may not have that choice, with the transposition of the General Data Protection Regulation (Directive 95/46/EC) (GDPR), CSPs typically store European data within the EU for compliance reasons. Notwithstanding this, a recent survey of 322 cloud TOS and privacy policies, suggested that 267 CSPs indicated that the US was the preferred jurisdiction, and specifically Californian law (Martic 2017).

Chapter 3 will discuss jurisdictional issues in greater detail, however it is important to highlight that choice of law can favour one side or the other in a cloud contract. For example, EU law does not allow the exclusion or limitation of liability to the same extent that US law might, and similarly the GDPR introduces significant responsibilities and penalties on data controllers and processors. Courts will consider a number of factors when deciding on the actual jurisdiction for a cloud contract including: (1) the choice of law in the TOS; (2) the nature and quality of the CSP's commercial activity in the jurisdiction; (3) whether the CSP is actively aware that they are making sales to client resident in a particular jurisdiction; (4) the jurisdiction that clients are resident or domiciled in; (5) the location where the cloud service is consumed; (6) the location whether the data is stored and processed; (7) the location of the CSP's offices; and (8) whether the CSP markets or solicits business in a given jurisdiction. If the answer to one or more of these questions is affirmative, a court may enforce jurisdiction.

In Europe, CSPs and enterprise clients often seek to use and rely on standard contract clauses, so-called EU model clauses, to manage data transfer outside the EU. However the applicability of these have been challenged in the recent case of *Data Protection Commissioner v Facebook Ireland (Schrems II)*. The judgment for this case was delivered in July

2020 with the CJEU largely following the advice of the Advocate General i.e. that model clauses should not be invalidated and that reliance on such clauses requires firms undertake additional measures to assure compliance. However, the CJEU, somewhat unexpectantly, decided to examine and rule the EU-U.S. Privacy Shield framework invalid thus requiring organisations relying on this mechanism to urgently consider and put in place alternatives.

2.4.2 Service Level Agreements and Limitation of Liability

The SLA outlines the CSP's commitments on availability, reliability, and performance levels for the specific cloud service contracted. These are typically presented as quantifiable targets for the standard of service, how such targets are calculated, mechanisms for auditing service delivery, and the level and procedure for compensation in the event of underperformance (Leimbach et al. 2014). The exclusions in SLAs can be quite broad and typically include an amount of scheduled downtime per annum (e.g. for maintenance) but also factors outside of the CSP's immediate control. Again, these are rarely negotiable on the grounds that the traditional cloud computing business model is based on multi-tenancy and commoditisation; negotiation is only available for those with significant bargaining power (Weber and Staiger 2014; Hon et al. 2012).

CSPs, reflecting a general practice in the wider IT industry, attempt to minimise their liability for any loss—direct, indirect, or consequential—that may arise from the provision of the service. In cloud computing, indemnities and liabilities are usually related to privacy and security breaches and resulting data loss, data misuse and associated regulatory penalties, but may also include service interruptions or outages, or otherwise failing to meet agreed service levels (Hon and Millard 2018; Leimbach et al. 2014; Bradshaw et al. 2013). It should be noted that CSPs, typically attempt to compensate, where possible, for underperformance through service credits. Obviously, this goes to the heart of trust, particularly where critical systems have been outsourced to a CSP. Trust literature suggests that trust repair is more effective when complemented with substantive actions including admission of fault and penance signals (Bachmann et al. 2015). However, in practice, it may be more nuanced. Where a cloud service is unavailable and business is adversely impacted, service credits for the same service are unlikely to be desirable or adequate compensation. Furthermore, CSPs will often seek to exclude a wide range of

under-performance and impose limitations on how service credits can be used (Bradshaw et al. 2011).

As discussed above, CSPs may try to achieve such limitations on their liability by specifying a preferential jurisdiction in the TOS. For example, US courts have enforced such limitations on liability for click-wrap agreements (see, for example, *Treiber & Straub, Inc. v. United Parcel Service, Inc.*). Given that the research referred to above suggests that consumers are not aware of the detail of the contracts they are agreeing to, and if they were, for the most part would still proceed, authors have suggested that the US courts should rejuvenate the doctrine of unconscionability to help cloud clients avoid waiving important legal rights (Calloway 2012). Notwithstanding this, EU law provides some protection against the exclusion of liability (see *GB Gas Holding v Accenture*). For individual consumers, the EU Unfair Terms Directive (Directive 93/13/EC) requires that contracts must be drafted in such a way to prevent the imposition of terms prejudicial to consumer rights. It introduces the notion of "good faith" in order to prevent significant imbalances in the dealing of consumers and suppliers. Article 5 of the Directive requires contract terms be drafted in plain and intelligible language and states that ambiguities will be interpreted in favour of consumers. Similarly, the EU Consumer Rights Directive (Directive 2011/83/EU) highlights the requirement for suppliers to provide specific information in a "clear and comprehensible manner." It also provides formal requirements and withdrawal rights for distance contracts. In 2022, new protections for consumers will be introduced as part of the Digital Content Directive (Directive 2019/770/EU) when they purchase digital services or digital content, or particularly relevant in the case of cloud services, when they exchange personal data that goes beyond the minimum necessary to provide the service. As a final comment, in Europe, data protection is a fundamental right set out in Article 8 of the EU Charter of Fundamental Rights. Article 82 of the GDPR provides for compensation for persons suffering damage due to unlawful processing or of an act incompatible with national data protection law.

2.4.3 Acceptable Use Policies

AUPs are typically incorporated or referenced in the TOS, and are used by CSPs, nominally, to protect themselves in the event of misconduct by their client, and their clients' end users. In effect, AUPs set out a largely homogenous list of prohibited activities and behaviours and the consequences for

misuse (O'Byrne 2019; Bradshaw et al. 2011). Common categories of prohibited activities include:

1. activities that engage in, foster, solicit or promote illegal, abusive or irresponsible behaviour e.g. fraud, hacking, hosting and distributing viruses, or abusive, offensive or morally repugnant content e.g. child pornography, excessive violence, hate speech etc.;
2. high risk use where the failure or fault of the cloud service could result in death or serious bodily or to physical or environmental damage e.g. use in air transportation, nuclear or chemical facilities;
3. non-consensual e-mail, advertising, tracking or other uses of personal data e.g. using cloud services to spam third parties with email or advertising; and
4. abusive or offensive behaviour towards a member of the CSP staff.

This is not an exhaustive list, yet one can see that many of these activities could preclude perfectly legal activities, e.g. healthcare, and many involve a judgment by the CSP, the basis of which is typically unclear. AUPs are often neglected by clients yet can result in suspension or termination of end user accounts or indeed the client's overarching agreement. Furthermore, CSPs often retain the right to vary the terms of the AUP independently of the main TOS. For enterprise clients, aligning their AUP and their CSP's AUP is critical, otherwise an end user may have an account terminated by the CSP while the enterprise client is still accountable for delivering the service (Hon et al. 2012). Ideally, enterprise clients should negotiate a process that may be more appropriate for their needs, e.g. that they, the enterprise client, should inform their end users of AUPs, end user account suspensions, or terminations. Hon et al. (2012) note that such negotiations would seem to be the exception rather than the rule.

2.4.4 Data Protection and Privacy Policies

Issues relating to data protection and privacy can be found in the TOS, SLA, AUP and, of course, the privacy policy. It is worth noting that the privacy policy often primarily relates to CSP collection and use of personally-identifiable data. Chapters 3, 4, and 5 discuss data protection and privacy in much greater detail, however three contractual aspects are worthy of note, namely data protection, data integrity and data availability.

CSPs are required to comply with data protection regulations. Under the GDPR, CSPs are typically "data processors" but may be "data

controllers" in their own right; similarly, CSP clients are typically data controllers. Article 32 of the GDPR requires the data controller and the data processor "to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…[including] measures to protect data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". Article 44 deals with transfers outside the EU and only allows such data transfer subject to the GDPR. Under the GDPR, the contract between a CSP and their client must stipulate that the data processor will only act on the instructions from the data controller. One area of potential friction is that of security. The extent to which a client can instruct a CSP on their security policies in a multi-tenant commoditized infrastructure is limited and CSPs have relied on adherence to industry certifications or best practice frameworks to overcome client and regulator concerns e.g. PCI-DSS, ISO27001, COBIT etc. At the same time, CSPs, typically reserve the right to change their security policies unilaterally (Leimbach et al. 2014). While such certifications are envisaged by the GDPR under Article 42, they are not obligatory. Being 'certified' does not equate to GDPR compliance; it merely certifies that the aforementioned technical and organizational measures are in place. Indeed, the issue of certification would seem to be an area still couched in ambiguity. The European Data Protection Board only issued guidelines on GDPR certification in June 2019 and it is unclear whether certification commonly cited by CSPs meets these guidelines at the time of writing (EDPB 2019).

Data integrity is often referred to but poorly defined. For example, there are ambiguities even between information and data integrity (Boritz 2005). Notwithstanding this, it is widely accepted that it is synonymous with representational faithfulness. In contrast, data availability is the extent to which an organisation's full set of computational resources are accessible and usable (Jansen and Grance 2011). Extant pre-GDPR research suggests that, at least historically, CSPs attempted to place responsibility for preserving data integrity and backup with the client (Bradshaw et al. 2011; Hon et al. 2012). Article 32 (1) of the GDPR requires data controllers and data processors to have the ability (1) to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and (2) to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. While the GDPR applies to personal data, this does not guarantee the integrity and availability of all data, for example non-personal business data, and only applies to data within the definition of the GDPR. As such, care should be

taken by organisations seeking to outsource operations to the cloud, particularly where one of the motivations is that the cloud is a safe way to back up data.

2.4.5 Variation in Terms

As referenced earlier, CSPs typically reserve the right to change contract terms and policies unilaterally. Such variation may be communicated by reference to an updated version of the TOS, the AUP, the SLA and the privacy policy on the CSP's website. This is particularly the case in consumer and free cloud services and can result in changes to the specific services being consumed or the service levels (Michels et al. 2019; Kamarinou et al. 2015; Hon et al. 2012; Bradshaw et al. 2011). In many of these cases, the only option for clients and end users is to take it or leave it. Clients may or may not be notified of changes.

2.4.6 Intellectual Property

A number of issues arise in relation to intellectual property (IP) rights that should be addressed in cloud computing contracts. Spulber (2018) posits that current contracts based on tangible services are not suitable for modern technological paradigms, such as cloud computing, as they neither fully recognise the complete spectrum of IP, exclusion of access, and transferability of non-rivalrous intangible assets, nor do they address problems that arise from intentional or unintentional cooperative contribution to the creation of intangible assets. Cloud computing raises significant issues in relation to the four main categories of IP, namely—trade secrets, patents, trademarks and copyright.

The complexity of the chain of service provision in cloud computing complicates IP management. In addition to the primary client outsourcing systems to the CSP, a wider number of stakeholders may be involved in the transport, processing and storage of data, many of which may not be privy to the initial agreement with the client. Excluding access to this data while meeting SLAs may not be feasible. This may result in inadvertent disclosure of trade secrets and confidential information generally and result in civil and criminal liabilities. In the case of patents, the distribution of confidential information relating to a proposed invention may constitute a form of public knowledge of prior art and can invalidate a patent. Given the opaqueness of the chain of service provision in cloud

computing, such an infringement may be difficult to prove. CSPs make use of a wide range of proprietary, third party and open source software in the delivery of their services, and will often attempt to exclude warranties on IP relating to such software, and particularly open source software (Hon et al. 2012). At the same time, AUPs will often include infringement of IP as a prohibited activity. Again, software indemnities tend to be one-sided in cloud contracts favouring the CSP.

Despite persistent rumours that social networking sites and other CSPs are attempting to claim rights in images loaded on to their systems, recent research suggests that CSPs do not seek to have copyright assigned to them but in many cases explicitly acknowledge that the end user retained the copyright (Michels et al. 2019). The ownership of metadata is less clear. Metadata is data about data and is often a by-product generated from the interaction of the clients and their end users with the cloud service. In this way, new data (which may be of value and therefore be an intangible asset) is created by the cooperation of the client, or their end users, and the CSP. While some data is used for cloud service optimisation, other data may be collected with no specific purpose in mind. This data, sometimes referred to as 'exhaust data' or 'digital data exhaust', may have significant value to third parties through data mining, aggregation or other data analytics techniques. Reed (2010) suggests that data generated by the CSP for its own internal purposes belongs to them, however if the data contains client data protected under copyright, the client may have an infringement claim—if the client is aware of such use at all. Reed (2010) suggests CSPs need to pay careful attention that they do not take unfair advantage of clients nor infringe copyrighted works. But what of digital data exhaust? Who owns this data? CSPs are typically silent on this. Indeed, it may be a case of 'don't ask, don't tell'. Nonetheless, contracts should state clearly whether such data is being collected and for what use.

Hon et al. (2012) identify similar issues relating to the ownership of software applications developed by clients or end users on a CSP's IaaS or PaaS platform where the CSPs integration tools are used or the software is designed for specific use only with that CSP's software, and is therefore tied to the CSP's IP. The emergence of cloud service brokerage (CSB) models, and in particular consumer app marketplaces (e.g. Google Play and Apple AppStore), B2B cloud application and API marketplaces (e.g. Salesforce AppExchange and RapidAPI), and indeed Marketplace as a Service models (Paulsson et al. 2016; Paulsson et al. 2020), complicate these matters further. In these cases, independent software vendors build

their businesses with near-total dependency on a small number of large cloud ecosystems where the underlying CSP holds disproportionate bargaining power and data. The degree of trust involved is near total. Similarly, where clients or end users suggest or actually implement improvements or bug fixes, it may not be clear where IP ownership lies (Leimbach et al. 2014).

2.4.7 Termination

Contracts may come to a natural and expected conclusion, or be unnaturally terminated due to breach of contract or some other event rendering them invalid. On termination, the contract should make adequate provision for the consequent handling of the client data including defining the term of service and (non-) renewal of service; termination events; data preservation; data deletion; and data transfer, following termination (Leimbach et al. 2014). The treatment of termination has legal and economic implications. CSPs can use data preservation, in particular, as a means of vendor lock-in by making data transfer to another service time-consuming or cumbersome. In the event of unnatural termination, clients will want to ensure that they have adequate time to access their data and transfer their data from the incumbent CSP to an alternative. At the end of a service contract, CSPs may (1) immediately delete the data, (2) provide a grace period, or (3) offer a hybrid approach neither obliging the deletion nor preservation of data, nor undertaking to delete data and offering a grace period at their discretion (Bradshaw et al. 2011). In reality, few CSPs delete the data on termination. However against the backdrop of data protection legislation, deleting personal data as soon as possible may be prudent to mitigate GDPR-related risk. At the same time, Hon and Millard (2018) have suggested that regulators are seeking maximum periods after which personal data must be deleted.

Leimbach et al. (2014) also note that clients should understand what happens to metadata relating to their account on termination; this issue would seem to be contentious not only from a termination perspective but also from an ownership perspective and is worthy of attention by cloud clients. As discussed above, the line between the metadata that a CSP reasonable owns and that which the client owns can be blurry and ownership uncertain. A CSP generates, stores, analyses and may replicate system and network usage, data transfer and other logs as part of the activities inherent in the delivery and future development of the service. It may not be

possible or desirable for CSPs to delete this data; similarly, clients may not wish inferences about them or their activities inferred from this data.

As a final comment on termination, while CSPs do not have a duty to make off-boarding easy or free, and indeed there is a palpable difference between the quality of on-boarding tools and support and off-boarding ones, they are not the only cause of delays. Customisation of cloud services, for example Salesforce.com, can result in both vendor lock-in and data portability issues. As such, cloud clients need to be aware of how integrated and dependent they are becoming on their CSP over time and the implications on termination.

2.4.8 Dispute Settlement

The overwhelming majority of CSPs include provisions for dispute resolution in their TOS however specific dispute resolution clauses may feature in other documents e.g. privacy policies (Martic 2017). CSPs may stipulate courts or arbitration to settle disputes and stipulate a choice of law in one or more jurisdictions (for example, see *Ryanair dac v SC Vola.ro srl*) or specific arbitration rules e.g. AAA or ICC rules. Research suggests that the preference is for courts as the exclusive adjudicative method (Martic 2017). As discussed previously, the determination of choice of law can favour one side or the other. For example, EU consumers can avail of the EU Alternative Dispute Resolution (ADR) Directive and the EU-wide Online Dispute Resolution (ODR) platform.

2.5 Future of Cloud Contracts

Current literature and thinking on contract law and cloud computing is based on relatively static conceptualisations of both cloud computing and contracts. The majority of legal research focuses on a conceptualisation of cloud computing from over a decade ago, primarily focussing on IaaS and SaaS services, and to a much lesser extent, Platform as a Service (PaaS). Recent work has suggested that the cloud is increasingly more abstracted, heterogeneous, composable, and automated (Lynn et al. 2020). First, the emergence of containerisation and serverless computing (including Function-as-a-Service) are enabling portability and a separation of concerns between CSPs and independent software vendors and clients (Lynn et al. 2020). These paradigms reduce vendor lock-in and create clear lines of demarcations between responsibilities and technology ownership in

ways not envisaged by traditional cloud computing. Similarly, cloud computing is becoming more heterogeneous and composable with a wider variety of customisable configurations available to clients that impact performance and complicate service level expectations, thus pushing performance-related decisions to the client, and requiring more nuanced agreements. Furthermore, with the advent of the Internet of Things, the cloud is becoming more decentralised and distributed across a cloud-to-thing (C2T) continuum. This has resulted in new computing paradigms including fog, mist and edge computing (Iorga et al. 2018). Processing and storage may take place in the cloud, at the edge or somewhere in between (the fog).

This new decentralised, abstract, heterogeneous, and composable cloud introduces complexity at several orders of magnitude higher than today. It is beyond human capabilities to manage such infrastructure manually. As a result, the cloud is becoming even more automated and intelligent. Artificial Intelligence for IT Operations (AIOps) algorithms and machine learning monitor, operate, and maintain distributed systems (Cordoso 2019). The emergence of self-organising and self-learning systems represents a significant evolution in cloud infrastructure decision-making. Outsourcing decision-making to AI provides substantial technical, legal and trust challenges, not least the black box nature of AI decision making. It is foreseeable that the actions of AI will result in cloud under-performance at some time in the future and addressed in accordance with existing legal provisions. However commentators have noted that AI may not be recognised as a subject of law, and as a result, may not be held personally liable for the damage it causes (Čerka et al. 2015). Cloud contracts need to evolve to reflect this changing and more nuanced cloud.

At the same time, the nature of contracts is developing, albeit at a much slower pace. Spulber (2018) has proposed a new framework for 'intellectual contracts', a form of "…agreement to create, develop, share, or apply intangible assets involved in technological change." In his conceptualisation, Spulber attempts to overcome the shortcomings of traditional contracts with respect to the completeness, excludability, and transferability of intangible assets while recognising that IP arises from intentional and unintentional cooperation, and rights in such outputs needs to be addressed in contracts. Similarly, there has been renewed discussions on the value of smart contracts in cloud computing with the emergence and hype around Blockchain. Smart contracts are not new; in effect they are agreements whose execution is automated and self-enforceable. Vending

machines are cited as common examples. In the mid-nineties, Szabo (1996) envisioned a computerised transaction protocol that implements the terms of a contract. While Szabo (1996) foresaw self-enforcing contracts based on conditions being met, Blockchain addressed a number of issues in smart contracts, and contracts more generally, not least the verifiability of conditions and performance. In the language of trust, Blockchain verifies integrity. Blockchain has been proposed as a solution to a number of cloud-related contract issues including verifiability of performance (Dong et al. 2017), GDPR compliance (Corrales et al. 2019), and digital rights management (Finck and Moscon 2019). Despite the benefits of smart contracts, significant questions remain unanswered regarding their enforceability (Savelyev 2017). Indeed, the extent to which either smart contracts or intellectual contracts can be easily adapted and integrated in to current contract law frameworks, or indeed need to, is open to debate.

2.6 Conclusion

This chapter provides an overview of some of the key contract law issues that arise in cloud computing. It is not exhaustive. It is clear that contracts in cloud computing are used primarily as an instrument of control and, to a lesser extent, coordination. While larger commercial and governmental organisations, may make rational choices based on calculus-based trust in full knowledge of the contract they are entering in to, it is clear that for the vast majority of firms do not have the opportunity or bargaining power to negotiate with cloud service providers. A rational, albeit disadvantageous decision, to either 'take it or leave it', remains. Given the homogeneous nature of cloud computing terms and conditions and the dominance of a small number of hyperscale players in the public cloud market, organisations, and particularly smaller ones, are left on the poorer side of a one-sided power relationship. While CSPs may possess undeniable competence, this imbalanced relationship does not foster trust. The evidence of the terms and conditions reviewed in this chapter suggest CSPs are not benevolent and their integrity can only be judged on their *post hoc* performance. Based on their approaches to limitation of liability, warranties, compensation, amongst others, one could understand how firms might tend towards scepticism. Such scepticism or lack of trust need not be a negative, it may be constructive resulting in enterprise customers developing healthy vigilance behaviours e.g. increasing monitoring, ensuring compliance, and preventing potential exploitation (Lumineau, 2017).

In contrast, individual consumers, by and large, do not make rational decisions with regards to entering in to contracts with cloud service providers. Research suggests that they do not read the terms and conditions in advance of using cloud services, and if they do, this does not change their decision. In this way, their decisions may be non-calculative and habitual, or reflect a perceived lack of options and/or a desire to avoid anxiety. At the same time, this is not their problem in one sense, but a regulatory one. There has been much progress to correct imbalances in contractual terms in consumer cloud computing, not least the GDPR. Unfortunately, regulatory responses are not uniform worldwide. Borderless technologies such as cloud computing provide significant challenges particularly in a highly globalised world. The rejuvenation of the doctrine of unconscionability as proposed by Calloway (2012) may be worthy of consideration, particularly in the US, the choice of law for so many cloud service providers.

Evolutions in cloud computing are overcoming the sources of legal friction between demand and supply. Containerisation and serverless computing introduce a separate of concerns that institutionalise a trust compartmentalisation of sorts in line with Lumineau (2017). At the same time, heterogeneity, AIOps, and the Internet of Things, further complicate the relationship between supply and demand, accountability and assurance, and as a result, trust and distrust. Innovations in contracts, whether intellectual or smart, remain at an early stage of conceptualisation. Indeed, it is unclear whether they are enforceable and can be adapted in to a legal infrastructure designed around traditional notions of tangible intellectual property and, even so, whether lawmakers will consider it necessary at all.

2.7 Cases

Caspi v. Microsoft Network LLC, 732 A.2d 528 (N.J. Super. 1999)
Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems (Case C-311/18)
El Majdoub v CarsOnTheWeb.Deutschland GmbH Case [2015] EUECJ C-322/14
Gas Holdings Limited v Accenture (UK) Limited and others [2010] EWCA Civ 912
Rudder v Microsoft Corp [1999] OJ No 3778 (Sup Ct J)
Ryanair dac v SC Vola.ro srl [2019] IEHC 239
Treiber & Straub, Inc. v. United Parcel Serv., Inc., No. 04-C-0069, 2005 WL2108081 (E.D. Wis. Aug. 31, 2005).

References

Bachmann, R., Gillespie, N., & Priem, R. (2015). Repairing Trust in Organizations and Institutions: Toward a Conceptual Framework. *Organization Studies, 36*(9), 1123–1142.

Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *The Journal of Legal Studies, 43*(1), 1–35.

Bellia, A. J., Jr. (2002). Promises, Trust, and Contract Law. *American Journal of Jurisprudence, 47*, 25.

Boritz, J. E. (2005). IS Practitioners' Views on Core Concepts of Information Integrity. *International Journal of Accounting Information Systems, 6*(4), 260–279.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology, 19*(3), 187–223.

Bradshaw, S., Millard, C., & Walden, I. (2013). Standard Contracts for Cloud Services. In *Cloud Computing Law* (pp. 39–72). Oxford: Oxford Scholarship Online.

Calloway, T. J. (2012). Cloud Computing, Click-Wrap Agreements, and Limitation on Liability Clauses: A Perfect Storm. *Duke Law & Technology Review, 11*, 163.

Čerka, P., Grigienė, J., & Sirbikytė, G. (2015). Liability for Damages Caused by Artificial Intelligence. *Computer Law & Security Review, 31*(3), 376–389.

CJEU (2019) - no longer required..

Cordoso, J. (2019). *The Application of Deep Learning to Intelligent Cloud Operation*. Paper presented at Huawei Planet-scale Intelligent Cloud Operations Summit, Dublin, Ireland, 1 November 2019.

Corrales, M., Jurčys, P., & Kousiouris, G. (2019). Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework. In *Legal Tech, Smart Contracts and Blockchain* (pp. 189–220). Singapore: Springer.

Dong, C., Wang, Y., Aldweesh, A., McCorry, P., & van Moorsel, A. (2017, October). *Betrayal, Distrust, and Rationality: Smart Counter-Collusion Contracts for Verifiable Cloud Computing*. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 211–227.

EDPB. (2019). Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en

Finck, M., & Moscon, V. (2019). Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. *IIC-International Review of Intellectual Property and Competition Law, 50*(1), 77–108.

Gartner. (2019). Market Share Analysis: IaaS and IUS, Worldwide, 2018. *Gartner*.

Hon, W. K., & Millard, C. (2018). Banking in the Cloud: Part 3–Contractual Issues. *Computer Law & Security Review, 34*(3), 595–614.

Hon, W. K., Millard, C., & Walden, I. (2012). Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now. *The Stanford Technology Law Review, 16*, 79.

IDC. (2013). *IDC Predictions 2013: Competing on the 3rd Platform*. IDC.

Iorga, M., Feldman, L., Barton, R., Martin, M. J., Goren, N. S., & Mahmoudi, C. (2018). *Fog Computing Conceptual Model*. (No. Special Publication (NIST SP)-500-325).

Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing*. SP 800-144.

Kamarinou, D., Millard, C., & Hon, W. K. (2015). *Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers*. Queen Mary School of Law Legal Studies Research Paper, p. 209.

Kimel, D. (2001). Neutrality, Autonomy, and Freedom of Contract. *Oxford Journal of Legal Studies, 21*(3), 473–494.

Lambert, R., & Peppard, J. (2013). The Information Technology–Organizational Design Relationship. In R. D. Galliers & D. E. Leidner (Eds.), *Strategic Information Management* (pp. 427–459). Routledge.

Leimbach, T., Hallinan, D., Bachlechner, D., Weber, A., Jaglo, M., Hennen, L., Nielsen, R. O., Nentwich, M., Strauss, S., Lynn, T., & Hunt, G. (2014). *Potential and Impacts of Cloud Computing Services and Social Network Websites*. Publication of Science and Technology Options Assessment.

Lumineau, F. (2017). How Contracts Influence Trust and Distrust. *Journal of Management, 43*(5), 1553–1577.

Lynn, T., & Rosati, P. (2017). Challenges to Technology Implementation. In M. Quinn & E. Strauss (Eds.), *The Routledge Companion to Accounting Information Systems*. Routledge.

Lynn, T., Rosati, P. & Fox, G. (2020). Measuring the Business Value of Cloud Computing: Emerging Paradigms and Future Directions for Research. In T. Lynn, J. Mooney, P. Rosati & G. Fox (Eds.), *Measuring the Business Value of Cloud Computing*. Palgrave-Macmillan.

Marotta-Wurgler, F., & Chen, D. L. (2012). Does Contract Disclosure Matter? *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft*, 94–123.

Martic, D. (2017). *Dispute Resolution for Cloud Services: Access to Justice and Fairness in Cloud-Based Low-Value Online Services*. (Doctoral Dissertation), Alma Mater Studiorum Università di Bologna. Dottorato di ricerca in Law, Science and Technology, 28 Ciclo.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review, 20*(3), 709–734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-commerce: An Integrative Typology. *Information Systems Research, 13*(3), 334–359.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. Gaithersburg, MD: National Institute of Standards and Technology.

Michels, J. D., Millard, C., & Joshi, S. (2019). *Beyond the Clouds, Part 1: What Cloud Contracts Say About Who Owns and Can Access Your Content*. Queen Mary School of Law Legal Studies Research Paper, p. 315.

O'Byrne, W. I. (2019). Acceptable Use Policies. *The International Encyclopedia of Media Literacy*, 1–6.

Paulsson, V., Emeakaroha, V., Morrison, J., & Lynn, T. (2016). Cloud Service Brokerage: A systematic Literature Review Using a Software Development Lifecycle. In 22nd Americas Conference on Information Systems, AMCIS 2016, CA, USA: San Diego.

Paulsson, V., Emeakaroha, V., Morrison, J., & Lynn, T. (2020). Cloud Service Brokerage: Exploring Characteristics and Benefits of B2B Cloud Marketplaces. In T. Lynn, J. Mooney, P. Rosati, & G. Fox (Eds.), *Measuring the Business Value of Cloud Computing*. Palgrave Macmillan.

Reed, C. (2010). *Information 'Ownership' in the Cloud*. Queen Mary School of Law Legal Studies Research Paper, p. 45.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not So Different after All: A Cross-Discipline View of Trust. *Academy of Management Review, 23*(3), 393–404.

Savelyev, A. (2017). Contract law 2.0:'Smart' Contracts as the Beginning of the End of Classic Contract Law. *Information & Communications Technology Law, 26*(2), 116–134.

Schwartz, A., & Wilde, L. L. (1978). Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis. *The University of Pennsylvania Law Review, 127*, 630.

Spulber, D. F. (2018). Intellectual Contract and Intellectual Law. *Journal of Technology Law & Policy, 23*, 1.

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. *EXTROPY: The Journal of Transhumanist Thought, 16*, 18.

van der Wees, A., Daniele, C., Jesus, L., Edwards, M., Schifano, N., & Maddalena, S. L. (2014). *Cloud Service Level Agreement Standardisation Guidelines*. C-Sig SLA, pp. 1–41.

van der Werff, L., Legood, A., Buckley, F., Weibel, A., & de Cremer, D. (2019). Trust Motivation: The Self-Regulatory Processes Underlying Trust Decisions. *Organizational Psychology Review, 9*(2–3), 99–123.

Weber, J. M., Malhotra, D., & Murnighan, J. K. (2004). Normal Acts of Irrational Trust: Motivated Attributions and the Trust Development Process. *Research in Organizational Behavior, 26*, 75–101.

Weber, R. H., & Staiger, D. N. (2014). Cloud Computing: A Cluster of Complex Liability Issues. *European Journal of Current Legal Issues, 20*(1), 1–13.