Cloud Computing:
A Practical Introduction to the Legal Issues
# Contents

**Acknowledgements**

<table>
<thead>
<tr>
<th>1</th>
<th>Foreword</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>History and development</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>What is cloud computing?</td>
<td>4</td>
</tr>
<tr>
<td>1.4</td>
<td>Cloud service types</td>
<td>5</td>
</tr>
<tr>
<td>1.4.1</td>
<td>SaaS – software as a service</td>
<td>5</td>
</tr>
<tr>
<td>1.4.2</td>
<td>IaaS – infrastructure as a service</td>
<td>5</td>
</tr>
<tr>
<td>1.4.3</td>
<td>PaaS – platform as a service</td>
<td>5</td>
</tr>
<tr>
<td>1.4.4</td>
<td>Utility computing</td>
<td>6</td>
</tr>
<tr>
<td>1.4.5</td>
<td>Grid computing or distributed computing</td>
<td>6</td>
</tr>
<tr>
<td>1.4.6</td>
<td>Other cloud service types</td>
<td>6</td>
</tr>
<tr>
<td>1.4.7</td>
<td>A stack of services</td>
<td>6</td>
</tr>
<tr>
<td>1.5</td>
<td>Deployment models</td>
<td>7</td>
</tr>
<tr>
<td>1.5.1</td>
<td>Public cloud</td>
<td>7</td>
</tr>
<tr>
<td>1.5.2</td>
<td>Private cloud (sometimes called an ‘internal cloud’)</td>
<td>7</td>
</tr>
<tr>
<td>1.5.3</td>
<td>Community cloud</td>
<td>7</td>
</tr>
<tr>
<td>1.5.4</td>
<td>Hybrid cloud</td>
<td>8</td>
</tr>
<tr>
<td>1.5.5</td>
<td>Consumer cloud</td>
<td>8</td>
</tr>
<tr>
<td>1.6</td>
<td>Technological terminology</td>
<td>8</td>
</tr>
<tr>
<td>1.6.1</td>
<td>Virtualization</td>
<td>8</td>
</tr>
<tr>
<td>1.6.2</td>
<td>Multi-tenancy</td>
<td>8</td>
</tr>
<tr>
<td>1.7</td>
<td>Comparisons with other types of IT services</td>
<td>9</td>
</tr>
<tr>
<td>1.7.1</td>
<td>Outsourcing</td>
<td>9</td>
</tr>
<tr>
<td>1.7.2</td>
<td>Managed services</td>
<td>10</td>
</tr>
<tr>
<td>1.7.3</td>
<td>Batch computing/service bureau</td>
<td>10</td>
</tr>
<tr>
<td>1.7.4</td>
<td>ASP – application service provision</td>
<td>10</td>
</tr>
<tr>
<td>1.7.5</td>
<td>Client/Server</td>
<td>10</td>
</tr>
<tr>
<td>1.7.6</td>
<td>Conclusion on differences</td>
<td>10</td>
</tr>
</tbody>
</table>
2 Which law of the cloud?

2.1 Introduction

2.2 International disputes as to applicable (cloud) law
   2.2.1 Yahoo! in Belgium
   2.2.2 Google in Brazil

2.3 Which law applies to the cloud?
   2.3.1 Introduction
   2.3.2 Data protection
   2.3.3 Contract law
   2.3.4 Liability issues
   2.3.5 Ecommerce Directive’s ‘Country of Origin’ rule

2.4 Law enforcement agencies’ ability to obtain data
   2.4.1 Introduction
   2.4.2 The US Patriot Act
   2.4.3 Application to the cloud

2.5 Key points

3 Information security

3.1 Introduction

3.2 Security breaches – some examples
   3.2.1 Sidekick
   3.2.2 Gmail
   3.2.3 Google Docs
   3.2.4 Google China
   3.2.5 Twitter breach
   3.2.6 Hotmail breach

3.3 Due diligence
   3.3.1 Introduction
   3.3.2 Security policies
   3.3.3 The customer’s enquiries
   3.3.4 The provider’s response

3.4 Introduction to security standards

3.5 ISO/IEC 27000 series
   3.5.1 Introduction to the series
   3.5.2 ISO/IEC 27001
4 Data protection: basics

4.1 Introduction
4.2 The basic structure of data protection law
4.3 Personal data
4.4 Data controllers and processors
   4.4.1 Introduction
   4.4.2 SWIFT
   4.4.3 Recent regulatory guidance
   4.4.4 Application to cloud computing
   4.4.5 Multiple controllers
4.5 Jurisdictional issues
   4.5.1 Introduction
   4.5.2 Established in the UK
   4.5.3 Established outside the UK
   4.5.4 Application of jurisdictional rules to cloud
4.6 The eight data protection principles
4.7 Legitimization of processing
   4.7.1 Personal data generally
   4.7.2 Sensitive personal data
4.8 Notification to the Office of the Information Commissioner
4.9 Enforcement
   4.9.1 Damages claims
   4.9.2 Enforcement notices
   4.9.3 Monetary penalties
4.10 How does all this apply to the cloud?
4.11 Key points
5 Data protection: appointing a cloud provider

5.1 Introduction
5.2 Cloud provider as a data processor
5.3 Cloud provider as a data controller
5.4 Pre-contract due diligence
5.5 Ongoing monitoring requirements
5.6 ICO’s views on cloud computing
5.7 Key points

6 Transfers of data to non-EU cloud providers

6.1 Introduction
6.2 Countries deemed automatically adequate
6.3 The US Safe Harbor
   6.3.1 Introduction
   6.3.2 The mechanics of Safe Harbor
   6.3.3 How are the Safe Harbor principles enforced?
   6.3.4 Limitations on the scope
6.4 Standard clauses
   6.4.1 Introduction
   6.4.2 Standard clauses in the cloud
   6.4.3 Onward transfers by the cloud provider
   6.4.4 Onward transfers when subcontractor is in a different country
6.5 Self-assessment
   6.5.1 Introduction
   6.5.2 Undertaking the analysis
   6.5.3 Self-assessment applied to the cloud
6.6 Binding corporate rules
6.7 Other derogations
6.8 Key points

7 Data security breach notification in the cloud

7.1 Introduction
7.2 The US position
7.3 Data breach notification in Europe
7.4 ICO guidance on data security breach management
7.5 Specific UK sectors
   7.5.1 Public sector
   7.5.2 FSA and other regulatory regimes
7.6 Application to the cloud 87
  7.6.1 Obligations upon the cloud customer 88
  7.6.2 Obligations upon the cloud provider 88
7.7 Key points 88

8 Software licensing and the cloud 90
  8.1 Introduction 90
  8.2 Moving existing licensing structures to the cloud 90
    8.2.1 Introduction 90
    8.2.2 Restrictions to be considered 91
    8.2.3 The provider’s risk 92
    8.2.4 Evolution of new licensing models 92
  8.3 Open source and the cloud 93
    8.3.1 Introduction 93
    8.3.2 Provision of software to a SaaS customer – the copyleft problem 94
    8.3.3 The viral effect in the cloud – the Affero Licences 95
  8.4 Software escrow in the cloud 96
    8.4.1 Escrow in a traditional environment 96
    8.4.2 Escrow in a SaaS environment 97
  8.5 Key points 98

9 Customer data: the provider’s use of data, access to data and lock-in 99
  9.1 Introduction 99
  9.2 The provider’s use of its customer’s data 99
  9.3 Access to data on exit 101
    9.3.1 Provider lock-in 101
    9.3.2 Commercial issues 102
    9.3.3 Technical issues 103
    9.3.4 Legal issues 103
    9.3.5 Contractual chains of cloud providers 104
    9.3.6 Lock-out and Coghead 106
  9.4 Key points 106

10 Service definition – the provider’s ability to change the service 108
  10.1 Introduction 108
  10.2 A comparison with software licensing 108
  10.3 From the provider’s perspective 109
  10.4 From the customer’s perspective 109
10.5 How to deal with service change in a cloud contract
10.6 Key points

11 Service levels
11.1 Introduction
11.2 Typical service metrics
   11.2.1 Availability
   11.2.2 Service response times
   11.2.3 Problem resolution times
   11.2.4 Elasticity
11.3 Availability
11.4 The consequences of missing service levels
   11.4.1 Target or contractual level?
   11.4.2 Credits and other remedies
   11.4.3 Calculating credits
   11.4.4 Exhaustive remedy
11.5 Standard exceptions
   11.5.1 Force majeure
   11.5.2 Third-party suppliers
   11.5.3 Customer
11.6 Drafting issues around SLAs
11.7 Termination for failure to achieve service levels
11.8 Key points

12 Liability issues
12.1 Introduction
12.2 Exclusions of liability
12.3 Limitations of liability
12.4 Chains of liability
12.5 Statutory and judicial control on liability exclusions
   12.5.1 Unfair Contract Terms Act 1977
   12.5.2 Unfair Terms in Consumer Contracts Regulations 1999
   12.5.3 Attacks on supplier’s standard terms
   12.5.4 The danger of overselling
12.6 Key points

13 Specific sectors
13.1 Introduction
13.2 Financial services
   13.2.1 Introduction to the regulatory regime
   13.2.2 Generally applicable rules – FSA Principles of Business
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.2.3 Banks, building societies and investment firms</td>
<td>135</td>
</tr>
<tr>
<td>13.2.4 Investment firms using cloud services</td>
<td>137</td>
</tr>
<tr>
<td>13.2.5 Insurance companies</td>
<td>138</td>
</tr>
<tr>
<td>13.2.6 Insurers using cloud services</td>
<td>139</td>
</tr>
<tr>
<td>13.3 Cloud in the public sector</td>
<td>139</td>
</tr>
<tr>
<td>13.4 Consumer cloud</td>
<td>140</td>
</tr>
<tr>
<td>13.4.1 Introduction</td>
<td>141</td>
</tr>
<tr>
<td>13.4.2 Liability of a cloud provider for hosting user content</td>
<td>142</td>
</tr>
<tr>
<td>13.4.3 Liability under contracts with consumers</td>
<td>146</td>
</tr>
<tr>
<td>13.4.4 Data protection with consumers</td>
<td>146</td>
</tr>
<tr>
<td>13.5 Key points</td>
<td>147</td>
</tr>
</tbody>
</table>

### 14 The future of cloud law

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1 Introduction</td>
<td>149</td>
</tr>
<tr>
<td>14.2 Open cloud</td>
<td>149</td>
</tr>
<tr>
<td>14.3 Development of industry codes of practice</td>
<td>150</td>
</tr>
<tr>
<td>14.4 Developments in data protection law</td>
<td>151</td>
</tr>
<tr>
<td>14.5 Commoditization of cloud services</td>
<td>152</td>
</tr>
</tbody>
</table>

**Glossary**

**Bibliography**

**Index**
To Annette and Max
Acknowledgements

I am indebted foremost to my clients on both the customer and provider side who I have advised over the years in relation to cloud services (sometimes, even before they were even called ‘cloud’). Thanks also to the many IT law and information security professionals with whom I have enjoyed discussing the issues covered in this book, including Amer Moorhead and his team at Ariba and John Moss at Salesforce.com, all of whom are involved daily in cloud law. Special mention should go to Andreas Fuchsberger of Microsoft, Christine Giraudon of Salesforce.com and Mark Watts of Bristows for their helpful comments on the manuscript, and likewise also to Dick Price of Beacon IT with particular thanks for his very expert comments on the ISO/IEC 27000 series section. Any errors are of course my own.

I would also like to thank my colleagues at Dechert (in particular, Paul Kavanagh and Kate Tebbutt) for support and encouragement. I also received useful help from the excellent trainee solicitors that passed through my supervision while the manuscript was being developed (Ailsa Fudge, Iria Giuffrida and David Lawne).

Thanks, above all, to my wife and son, Annette and Max, for their love and support and for their understanding as to the time commitment involved in writing this book; and especially to Max for choosing the cover.

Lastly, my thanks go to all at BSI especially to my editor, Julia Helmsley, for her experienced guidance to a first-time author, to David Fatscher for his initial suggestion that we collaborate on this book and to Siobhán FitzGerald for steering it through production.
1 Foreword

1.1 Introduction

There is no universally accepted definition of ‘cloud computing’ and the term means various things in different contexts and indeed to different people. It is a paradigm shift in how computer resources are acquired. Some doubt that there is anything new about the cloud, pointing out the fact that many of the features which are said to be part of this paradigm have in fact existed for quite some time in other (non-cloud) technologies and services.

A fuller definition of the terminology necessary to serve the aim of this book is set out further on. However, in summary, cloud computing refers to the delivery of computing capability (whether of an application software variety, an infrastructure delivery, or otherwise) by a provider remotely over a communications link, allowing for no actual installation (of the software or the infrastructure) at the customer site.

It is not only enterprises that are using cloud services. The history of the consumer cloud is intimately linked to the history of the internet. Many common and well established web services such as email services (e.g. Hotmail) and photo sharing services (e.g. Flickr) have existed since the early days of the web, but over the last few years the willingness of consumers to trust often quite sensitive personal information to social networking sites (Facebook, LinkedIn and others, all of which are ‘cloudy’ in nature) has taken the trust to a new level.

This book attempts to identify, discuss and elucidate many of the common legal issues that arise from this paradigm shift. It is intended to be practical and assumes very little by way of legal knowledge. In respect of the more difficult legal issues (such as perhaps data protection and security), a practical understanding necessarily depends on a fuller exposition of the underlying law – which is provided – but again it is hoped that the end result is nonetheless useful to those not legally qualified.

One of the problems with analysing cloud issues from a legal perspective is the multinational aspect: the fact that many countries may be involved in a particular cloud provision. A customer in country A, for example, may use a SaaS (software as a service) offered by a provider in country B, who in turn acquires infrastructure
capacity in countries C, D and/or E (depending on the current price in each).
Whilst this book is based on English law, many of the issues which arise (in particular in relation to risk allocation and service provisions in contracts) will be common across different legal systems. The issues surrounding data protection discussed in chapters 5 to 7 are very similar throughout Europe as a result of a common adoption of the same Data Protection Directive [1]. Issues such as service description (chapter 10) and service levels (chapter 11) are matters of technical capability, business assessment, negotiation and risk, and are largely independent of the law of the country in which either the customer or the provider reside. As such, non-UK readers may also find it interesting.

Whilst this book is intended as a practical guide to these issues, it goes without saying that it is no substitute for considered legal advice.

1.2 History and development

For present purposes, the history of computing could perhaps be summarized as follows:

a) 1940s: early beginnings in isolated research centres;
b) 1960s to 1970s: mainframe computers and dumb terminals; bureau processing;
c) 1980s: the rise of the PC and Microsoft; standardization of hardware; the rise of independent software vendors; commencement of large scale outsourcing;
d) 1990s: the advent of networking and the internet; .com boom; application service provision;
e) 2000s: .com bust; the distribution of ever-increasing accessibility through broadband and Wi-Fi; the rise of Google and the consumer cloud;
f) 2010s: virtualization; green-computing; the rise of the business cloud (perhaps).

As this very approximate time line is examined, it is possible to detect a number of characteristics relevant to why the cloud is happening now. First, it is notable that in the early days of computing, hardware manufacturers were the dominant players, and software languages were tailored for specific machines. Computing power was concentrated in the few and the idea of processing data through a remote service (a bureau service) was not controversial (as it is now), simply often a necessity. As time progressed, it was possible for entities to handle internally their own IT requirements and the in-house IT department was born. Time moved on again and it was recognized that that is not often very efficient. Computing could be left to the experts and outsourcing (in many guises) began. Cloud computing can be seen as just one type of outsourcing, and indeed there are some who consider there
to be little difference between what is now labelled ‘cloud’ and what went before and that there is simply a hype surrounding it.

Larry Ellison, the CEO and founder of Oracle, for one, has been very critical of the surrounding hype. He has given a number of widely quoted interviews, including one in 2008 in which he made the point that the definition is so wide that it includes everything that Oracle actually does, comparing it disparagingly to women’s fashion and referring to it as ‘complete gibberish’.\(^1\)

In the same interview, he also makes the point that all these predictions about how things would change are so often wrong. The PC would kill mainframes; they did not. Open source software would kill software houses; it has not.

Others, implicitly recognizing that there is something new happening, are critical of the movement. Richard Stallman, the founder of the GNU project and open source software pioneer, has called cloud computing ‘stupidity’ – a means for the gullible to be locked into particular providers (once those providers have the user’s data in a proprietary format). The issue of provider lock-in is explored in chapter 9.

Whether or not there is a real paradigm shift might depend on the type of cloud service that is being talked about. As the brief timeline shows in this clause, the idea of obtaining use of a software application remotely is as old as computing; early software use involved access to mainframes with distributed dumb terminals or to data processing power through bureau services. So, in a sense, at least one of the types of cloud services (SaaS) might be nothing particularly new from what has gone before but with one important distinction – the distinction of scale. It has simply become more prevalent. As such there is at least a germ of truth in what Larry Ellison says: much of it has been done before. Other types of cloud offering, for example, the idea of acquiring server capacity in a ‘utility-like’ manner (IaaS – infrastructure as a service), paid for as you go and scaled as you need, may well represent a fundamental shift in the acquisition of technology motivated by many concerns: cost pressures, economies of scale, energy efficiency.

More pertinent perhaps is the issue not so much of whether this is hype but rather – even if it is hype – why it is happening now. Arguably, it is happening now because it is a real phenomenon driven by a desire to minimize computing costs, have flexibility and be more efficient – a desire matched by IT providers tailoring their offerings on the back of easily accessible high-speed connectivity through the internet and otherwise.

It seems likely that, new or not, the cloud is here to stay.

\(^1\) Larry Ellison, Oracle OpenWorld, 25 September 2008.
1.3 What is cloud computing?

There are many different views on the question, including much academic, technical and business disagreement as to what the salient features are. For present purposes, broadly, cloud computing refers to the delivery of computing capability by a provider remotely over a communications link. It comes in many different varieties, serving a wide variety of computing needs, and there are inevitably arguments and discussion over what are the essential elements of a cloud offering. The following are the most important features which trigger the application of legal issues dealt with in this book. A typical cloud offering will involve (some if not all of) the following features:

a) there will be no actual requirement for software installation at the customer site (except for a standard internet browser);

b) the customer will be using software operated by the provider on servers controlled by the provider (or on behalf of the provider);

c) the customer can pay on a usage basis;

d) the delegation to the provider of responsibility for keeping software up to date;

e) the delegation to the provider of responsibility for keeping data secure; and

f) the delegation to the provider of responsibility for managing the hardware.

This list is not set in stone and not all of these features are essential; many offerings that are properly called cloud may omit one or more. Some would argue that the list is in fact too short and, for example, that an important feature of a genuine cloud offering is that there is in fact no clearly allocated server for a particular customer and/or that different customers are serviced using the same ‘instance’ of the software in a multi-tenancy model. Where a particular feature's presence or absence is important to a particular issue which is covered in this book that will be made clear.

A basic categorization is between on the one hand a cloud service that provides use of software remotely and on the other hand a cloud service that provides use of hardware or other infrastructure components. The next sections explain expressions that are frequently used to describe some of the different aspects of cloud. Some identify the type of service, others the deployment models of the service, and lastly some identify different technologies involved.
1.4 Cloud service types

A number of terms are frequently used to describe the cloud service types as follows.

1.4.1 SaaS – software as a service

The quintessential cloud offering: application software is no longer downloaded or installed onto the user’s computer (server or PC) but instead is provided remotely by the provider, perhaps through a web interface. It is subscribed to, not licensed.

There are a myriad of examples, perhaps the most-quoted one being Salesforce.com’s Customer Relationship Management (CRM) service.

1.4.2 IaaS – infrastructure as a service

The idea here is that the hardware (or other infrastructure) needs of an organization are met remotely by the provider. The provider takes responsibility for the customer’s processing needs, normally of servers but perhaps also of storage devices. Web hosting services (where a company’s websites would be hosted by a specialist company) have always been, in a sense, a very simple type of IaaS – a server being provided for the specific need of giving the customer a web presence. However, that concept has now evolved so that the servers on which the site is hosted will be ‘virtual’ and ‘scalable’. In this regard, a term that is often seen is ‘cloud hosting’, a type of IaaS, providing the benefits of scalable, on demand, and – say the providers – low-cost web hosting to many companies.

IaaS is wider than simply web hosting. The widest variety of hardware and for the widest range of uses is available. Amazon’s cloud offerings are prominent examples: Amazon’s Simple Storage Service (Amazon S3) provides a cloud storage service whilst its Elastic Compute Cloud (Amazon EC2) provides server capacity.

1.4.3 PaaS – platform as a service

This is IaaS with added value designed to allow smaller providers quickly and cheaply to set up SaaS services. A potential provider of a SaaS service will of course still need infrastructure upon which it can operate its software for its customers. It could take a two step approach: first, develop its own software in a traditional manner and then, secondly, deploy it on an IaaS offering acquired from elsewhere. A PaaS solution brings these two steps together. An additional layer (the ‘platform’) of software is provided over and above the infrastructure that appears in IaaS. This platform allows the customer to develop its own software.
application (with the provider’s development tools) and deploy that software application through the infrastructure. Whilst clearly of immense use to smaller businesses keen to set up a cloud business with minimal effort and investment in more traditional development tools, an overriding issue for many in using this type of offering is the fact that the application thus developed will then only be capable of running on that particular cloud platform. There is therefore a particular and pronounced issue of vendor lock-in. Prominent examples are Google App Engine and Microsoft Azure.

1.4.4 Utility computing

The idea behind utility computing is that computing technology can be switched on and off in much the same way as electricity and other utilities. For the purpose of this book, the term adds little to what is included within the term ‘IaaS’.

1.4.5 Grid computing or distributed computing

This is a type of computing network where the capacity of a large number of computers accessed through a network is available to particular types of users. University and scientific computing capacity is often structured in this manner so that heavy processing tasks (e.g. meteorology) can make efficient use of vast computing resources when they might otherwise be idle. Another example of this, which has captured the popular imagination, is the Search for Extraterrestrial Intelligence (SETI@home) project, where a great quantity of data from radio telescopes gathered by astronomers is sent out to numerous home computers. The software on the home computers runs when the screen saver is on (or is otherwise idle) to try and detect patterns in the data which might indicate extraterrestrial life.

1.4.6 Other cloud service types

The computing industry seems to know no bounds in creating new ‘aaS’ terms, and the following are all beginning to appear in literature: business (or Business Process) as a service (BaaS), storage as a service (StaaS), desktop as a service (DaaS) and so on.

1.4.7 A stack of services

Figure 1 illustrates how different types of providers can in fact ‘sit on top of each other’. An understanding of the existence of this stack is important as it determines, for example, where in fact the customer’s data might be. The customer will ordinarily only contract with one party; when it is acquiring a SaaS service, it will only contract with the person at the top of the diagram. The data might however be in the actual possession of the IaaS provider (and, to complicate matters, there could be a subcontractor below that provider).
1.5 Deployment models

There are terms that define the type of person to whom a particular service is deployed (whether SaaS, PaaS or IaaS):

1.5.1 Public cloud

Most cloud services are used by anyone willing to acquire them, and this is what is meant by a ‘public cloud’ offering.

1.5.2 Private cloud (sometimes called an ‘internal cloud’)

Some aspects of cloud computing can be adopted without involving an external provider. A private cloud is when cloud-like services are deployed within a large group, say, by a dedicated service company providing software or infrastructure services remotely that is usable by any of the members of that group. Some commentators would add a requirement that there must also be dynamic availability (depending on demand) of applications or resources before the offering is truly a private cloud. For some organizations, a private cloud may initially be a stepping stone on a transition path to use of a full cloud offering.

1.5.3 Community cloud

A cloud service used by a specific group of persons (the members of a particular community).
1.5.4 Hybrid cloud

When an organization uses more than one type of cloud (or more than one offering from different cloud providers), they are using a hybrid.

1.5.5 Consumer cloud

Many of the services used by consumers on the internet are cloud services. Social networking sites involve the consumer storing their (sometimes very) personal data on services under the control of Facebook, Bebo, LinkedIn and the like. Likewise, email services such as Hotmail and Gmail are true cloud services. Of course, consumers do not use those expressions and do not generally consider such issues as data security and server location.

1.6 Technological terminology

The cloud model brings with it a number of technical terms (describing particular technologies which may feature in different services or deployments) which will need to be understood by those navigating the legal issues.

1.6.1 Virtualization

This term normally describes a technology under which software that an enterprise needs runs not on a specific server, but on a ‘virtual’ server. Many IaaS services depend on this technology (but they are not synonymous). The virtual server might be spread across a number of different physical servers, and the IT infrastructure manages the load (dynamically and invisibly to the applications themselves and certainly the users) to ensure that the most efficient use of the underlying physical computing power is made. The term can also cover the reverse situation where a number of different virtual servers operate on one physical server. Whilst common in IaaS offerings, a virtualized infrastructure can also be implemented by the enterprise’s own IT department (perhaps as part of a private cloud).

Virtualization software exists for home consumers’ use also, allowing the host desktop to appear as a number of different virtual PCs.

1.6.2 Multi-tenancy

This is a term that describes how a particular ‘instance’ of software running on a server (or servers) is used by the cloud provider to provide services to many of its customers. It is an important concept as it appears time and time again in contract negotiations in relation to cloud offerings; in particular, it will often be used by service providers to justify many of the stances they take in their contract terms.
The basic idea is that the same copy of the software is running data for many customers at the same time.

Given the importance of the concept, a further word of explanation might be helpful for the non-technically minded. In a traditional deployment of software, when software is run on a computer internal to an organization (this is a simplification), one copy of the software is brought into the memory of the computer (from the hard drive) and that copy accesses and processes that organization’s data. That is one ‘instance’ of the software in memory. Another customer using the same software may well be using the identical software (in the sense of same version number) but it will be a different instance (not least because it is on a different computer).

Now assume that the software is provided remotely by a SaaS provider. The provider might run the same program a number of different times (multiple instances) concurrently on the same server; each instance would process different data for different clients. However, it would also be possible for the provider to run just one instance to simultaneously process two different sets of data (for two different clients). Each set of data in this scenario is a ‘tenant’ in the instance, hence ‘multi-tenancy’. Naturally, as the two sets of data might belong to separate clients, security and a proper segregation of data within the one instance is paramount.

1.7 Comparisons with other types of IT services

Cloud computing may well be new, but various aspects of this model do feature in other more traditional types of IT offerings – from the recent past (out of which cloud may have in part evolved) but even from the more distant past. As such, many of the legal issues that arise in cloud will be familiar from these other scenarios. With that in mind, and with a view of applying legal principles which had been applied to these other types of IT offerings, it will be useful to identify similarities and differences between cloud computing and those offerings with which cloud shares features.

1.7.1 Outsourcing

Outsourcing involves the handing over of an IT function previously provided internally to an external provider. It might involve the outsourcing of the whole IT department (data centres, all support staff, in–house development teams, and so on) but might be more limited. It can be similar both to IaaS (as the provider will manage the infrastructure) and to SaaS (as software functionality may be served to the customer remotely). The provider will of course have to handle security. It might also (depending on what is outsourced) involve the creation of applications and the delivery of software to users and so be similar to PaaS.
1.7.2 Managed services

This is a type of outsourcing where servers and software are managed remotely from the customer by the service provider. Similar in some instances to an IaaS service, the provider will provide remote access to the service, manage the infrastructure, and have actual possession of data. It does not necessarily involve (but can have) virtualization. When there is virtualization, it can have usage charging models. The location of the data centre is usually known.

1.7.3 Batch computing/service bureau

An example from the earlier days of computing, this is the provision of remote data processing by dedicated software on servers. Customer data is input, processing is carried out, and data returned to the customer (or action undertaken). Similar in some instances to a SaaS service, data is held by the provider and the provider keeps software up to date. Again, the location of the data centre is usually known.

1.7.4 ASP – application service provision

A term (from the late 1990s and early 2000s) that has somewhat fallen out of fashion, but in essence is simply SaaS. An application is provided as a service remotely.

1.7.5 Client/Server

A software architecture that divides processing between a client (or clients), which requests the service, and a server, which fulfils them. It is similar (and an early precursor) to SaaS, at least when the architecture is used externally. When used internally, it is similar to SaaS on a private cloud. Normally, the server and client side are managed by the same person and that is perhaps a distinction to be drawn.

1.7.6 Conclusion on differences

As can be seen, therefore, many cloud features existed in pre-cloud days (so maybe Mr Ellison is right). The one feature that is definitely new is that which – as we will see – presents the greatest difficulty: the customer does not necessarily know where the data is. Other parts of the paradigm are familiar with, and the legal issues that arise are similar to, what has gone before. Data is held by a provider who takes care of security, service level commitments are necessary, and so on.

1.8 Why now?

Whilst it is probably true that SaaS has been around for a while, there are a number of reasons as to why the concept of cloud computing has attracted such traction recently. First, the size of the players involved means that anything they
do will have serious and widespread repercussions. Amazon (and its like) has built such large data centres, literally the size of many football pitches, to fulfil its requirements. Naturally its requirements for IT resources vary over time with peak demand, in particular, around Christmas (in common with many retailers). But it is not just around the holidays; demand varies throughout the day and over the week. Amazon identified that it had to do something with its spare capacity and began in 2006 to offer that capacity to other businesses through its Amazon EC2 service, allowing them to acquire infrastructure on a pay as you go model. Where Amazon led, many other IT giants (Google and Microsoft) followed.

A second reason as to why there is at present such an acceleration into the cloud is the recognition by many users of technology of the wastage in their own server capacities, and thus a drive towards the saving of costs. Linked to the cost saving is the current green agenda and a move towards ‘green computing’. This latter term aims to identify an imperative to be more eco-friendly in sourcing computing power. It has been estimated that a typical business is wasting at least 75% of the capacity it has for storage and 85% of the capacity it has for processing power. Sharing resources is a way of more efficiently using computing technology.

Thirdly, the Amazon model allows very large economy of scale and that too has had a major impact when IT budgets increasingly take a bigger share of a company’s cost base.

Lastly, it is quite simply becoming technically possible. Broadband is widespread and now reliable, leased lines are prevalent, and it is ever easier for businesses to make the leap and trust the remote provision of services.

1.9 Overview of this book

This book is intended to be a practical introduction on legal issues in cloud computing suitable for those either providing such services or considering an acquisition. It is designed to be read as a practical introduction and the hope is that it will be of interest to lawyers and non-lawyers alike, anyone navigating the difficult legal issues which might arise. Where the legal issues arising depend on some background knowledge, not much is assumed. Instead, a short introduction is provided so as to make this as self-contained as possible.

In any cloud situation, in order to navigate the various legal issues that arise, it is important first to identify the relevant body of law that applies. We address this issue in chapter 2.

The next series of chapters deal with information security (chapter 3) and then data protection in chapters 4 (basics), 5 (putting personal data into the cloud), 6 (moving personal data outside of Europe) and 7 (data breach notification).
We then move onto issues that arise as a result of contracts. Chapter 8 deals with software licensing issues (including issues around moving legacy systems onto cloud infrastructures and open source). In chapter 9 we deal with a number of issues relating to customer data. Sometimes providers want to use data for their own purposes; this can be controversial and is explored here. It also covers the critical issue of customer lock-in and access to data. Chapter 10 covers issues relating to definition of the service and the ability of the provider to change the service, whilst chapter 11 deals with service levels and service credits. A provider’s ability to limit its potential liability by contractual language is dealt with in chapter 12. In chapter 13 we move to issues that arise in specific sectors (financial services, the public sector and consumers). Finally, in chapter 14 we look to the future of cloud law.

1.10 Contracting for the cloud

One further point should be noted at this stage. Throughout this book we discuss how a contract might deal with a particular issue to address a concern of the customer and how the customer might want to critically review language suggested by the provider. Implicit in this discussion is the idea that the provider will entertain a request that the contract be negotiated. It is worthwhile exploring therefore the extent to which contracts are being negotiated.

One aspect of cloud computing which is often cited as being different from other outsourcing deals is the take-it-or-leave-it aspect of the provision. In keeping with the commercial and technical advantages of the solution being easy to set up, easy to scale, and easy to control charges, it is also equally easy to contract: a customer simply accepts the provider’s terms without question. This is very true in relation to many provisions available at relatively low cost and possibly without any interaction except through the provider’s website. It is not however true of substantial acquisitions by enterprises. Contracts are still individually negotiated. Many cloud providers may present their contracts as standard and not invite negotiation. Nonetheless, customers can request changes to the ‘standard’. Whether the provider agrees to those requests will depend on the negotiating power of the customer. Consumers and most small businesses, each acquiring a very standard cloud offering, will have no scope for negotiating terms. That is not the case for substantial enterprises negotiating as equals with a cloud provider. The bigger the potential contract, the greater the scope for the cloud provider moving from its standard position to secure the deal.