Cloud Computing and Data Sovereignty
Richard Kemp
October 2015
CLOUD COMPUTING AND DATA SOVEREIGNTY

TABLE OF CONTENTS

Para | Heading | Page
--- | --- | ---
A. | INTRODUCTION | 1
1. | What is data sovereignty? | 1
2. | Cloud computing: the NIST definition | 2
3. | Current growth of cloud computing | 3
4. | Data sovereignty and cloud computing: the ‘privacy v intrusion’ debate and managing risk | 3
5. | Aims and scope of this white paper | 4
B. | DATA SOVEREIGNTY IN THE NEWS | 4
6. | Introduction | 4
7. | The Snowden allegations | 5
8. | Schrems v Facebook | 6
9. | Microsoft v United States: In re Warrant etc. | 9
10. | The UK Data Retention and Investigatory Powers Act 2014 (DRIPA) | 10
11. | Upcoming review of UK telecoms and internet surveillance laws | 11
C. | DATA SOVEREIGNTY: LEGAL BACKGROUND | 12
12. | Data sovereignty and the state’s investigatory powers: introduction | 12
The State’s Powers
13. | The framework of investigatory powers under UK law | 12
14. | The framework of UK data interception and collection: RIPA and DRIPA | 14
15. | The extra-territorial reach of UK data interception and collection law | 15
16. | Extra-territorial reach: other countries’ laws | 16
17. | A trend towards data residency, localisation and domiciliation laws | 17
18. | Mutual Legal Assistance Treaties (MLATs) | 17
19. | Legal Professional Privilege (LPP), etc | 18
CITIZEN’S RIGHTS
20. | No right to privacy at common law: non-applicability to communications of the 1760s warrant cases | 18
21. | Right to privacy, etc under the ECHR, EU Charter and data protection legislation | 20
D. | DATA SOVEREIGNTY AND CLOUD COMPUTING: SPECIFIC ISSUES AND PRACTICAL RISK MANAGEMENT | 22
22. | Data on-premise and in-cloud: isolating specific cloud computing data sovereignty issues | 22
23. | Cloud SPs and data sovereignty issues | 22
24. | CSCs and data sovereignty issues: contracting with the Cloud SP - investigatory powers, regulatory access, etc | 24
25. | Consumers | 26
26. | Practical risk management: data governance and contract | 26
27. | Data governance | 27
28. | Contract | 28
E. | CONCLUSION | 29
29. | Conclusion | 29

TABLES, ETC

Figure 1: Software as a Licence to Software as a Service: the Cloud Service Model Continuum (page 2)
Glossary (page 30)
CLOUD COMPUTING AND DATA SOVEREIGNTY

A. INTRODUCTION

1. What is data sovereignty? The migration of computing to the cloud is raising novel legal issues around data as processed and stored in-cloud and as transited between user and cloud service provider. These evolving cloud data legal issues principally concern data rights, data protection (privacy), data security and data sovereignty. For lawyers specialising in the field these issues arise most frequently in the areas of regulation, contract and governance.

Data sovereignty distinguished from data rights, protection and security. From the cloud customer’s perspective, there may be little apparent difference between data sovereignty (on the one hand) and data rights, data protection and data security (on the other). Whilst all four areas overlap, data rights (the intellectual property and other rights that arise in relation to data), data protection (the legal rights and duties that arise specifically in relation to personally identifiable information) and data security (the mix of management, legal, technical, operational and governance controls that an organisation puts in place to ensure desired security outcomes for its data) are separate topics and not considered in detail here except as relevant to data sovereignty.

Elements of data sovereignty. Data sovereignty does not have a generally accepted defined – it is not even mentioned in any of the three recent UK surveillance-related reviews referred to at paragraph B.11 below. The term bears an intuitively understood meaning of when a person’s right to deal as she or he wishes with her or his own data may be overridden, typically through involuntary disclosure to or access by a third party. This can arise of course if the person was using data in breach of someone else’s contract, intellectual property or other rights or other applicable legal or regulatory duties, but a bit more analytically data sovereignty may be considered as the circumstances in and extent to which:

- a third party (typically but not always a government agency);
- has the power to access the data of another person (the corporate or individual customer);
- where that data is in the possession of the customer or someone else on the customer’s behalf (the cloud service provider);
- with or without the consent or knowledge of the customer and/or the cloud service provider.

Data sovereignty on-premise and in-cloud. This could happen to data on-premise (on a personal device or in the server room for example) as well as in-cloud, and this paper focuses on data

---

1 All URLs referred to in footnotes were accessed in between 5 July and 6 October 2015.
Data sovereignty issues particular to the cloud – whether in transit to or from, or stored or processed in, the cloud.

**Data sovereignty viewpoints – government, Cloud SPs, CSCs and consumers.** Data sovereignty affects four main types of actor - government, cloud service provider and corporate and individual cloud customer - and relevant issues differ for each. Government agencies are concerned principally with the scope of their data access powers, how those powers are authorised, and accountability for their use. For cloud service providers (**Cloud SPs**), the big issues are around trust and reputation in the market, and operationally around contract terms, policies and governance. For cloud service customers (**CSCs**) the issues are broadly similar to those for providers and generally obverse to them in contractual and policy terms. CSCs are concerned mainly about the security of their data – looking at trust from the other end of the telescope. This paper focuses on cloud data sovereignty as it concerns commercial actors in the value chain – Cloud SPs and CSCs.

2. **Cloud computing: the NIST definition.** Briefly, the classic NIST definition⁴ of the cloud specifies a type of computing with five key characteristics, three service models and four deployment models. The characteristics are on demand self-service, network/internet access, one-to-many provisioning (resource pooling or demand diversification), rapid scaling (elasticity) and measured (metered) service; the elements of the **SaaS**, **PaaS** and **IaaS** service models are shown at 1, 2 and 3 in Figure 1 below; and the four deployment models are **private cloud** (where infrastructure, platform and/or software are used solely for a single CSC), **community cloud** (solely for use by a community of CSCs, rather than a single CSC), **public cloud** (where service is provided to customers on a multi-tenant basis) and **hybrid cloud** (private cloud with access to public cloud to manage peaks).

---

*Figure 1: Software as a Licence to Software as a Service: the Cloud Service Model Continuum*

---

3. **Current growth of cloud computing.** The growth of cloud computing is driven by a number of factors, chief among which is price. At scale, and after a large user has taken the first step away from on-premise to private cloud, the price premium of private over public cloud is around ten times:

“For large [users] with an installed base of approximately 1,000 servers, private clouds are feasible but come with a significant cost premium of about 10 times the cost of a public cloud for the same unit of service, due to the combined effect of scale, demand diversification and multi-tenancy”.

Driven by these factors, cloud computing is currently at an inflexion point and by late summer 2015 has become the ‘new normal’. Quarterly results published in July 2015 from Microsoft and Amazon, two of the top four cloud service providers, show cloud service revenues at each company almost doubling year on year to account for nearly ten percent of total revenues. This growth is still towards the start: according to research firm IDC, spending on public cloud computing services will grow by twenty-three percent on average each year from 2014 ($57bn) to 2018 ($128bn), with SaaS growing from $40bn to $83bn and PaaS and IaaS together growing from $16bn to $45bn.

4. **Data sovereignty and cloud computing: the ‘privacy v intrusion’ debate and managing risk.**

Despite the quickening pace of cloud computing growth, the significance of cloud data issues is amplified currently by reverberations from the Snowden allegation and by debate and litigation about the balance between citizens’ rights to privacy and the state’s powers to intrude. This has fuelled anxiety in the business world and among consumers about ‘my data in your data centre’, in turn heightened by regular news stories about hacking (whether of on-premise or in-cloud systems).

The ‘privacy vs intrusion’ debate has generated as much heat as light and is likely to get fiercer in the UK as we go into 2016. In order from a practical point of view to help put into context and refine the steps that businesses may take to mitigate the data sovereignty risks highlighted in this paper, it is probably worth bearing in mind two points from the outset. First, although the Snowden revelations centred on the USA, the alleged state surveillance and data intrusion powers are generally thought likely to exist across the world. Second, at root, government sees them as the contemporary expression of powers to keep the country safe that have existed since time immemorial so there is an element of business having to learn to live with them and manage the risk. These factors combine in the commercial world to support a pragmatic approach to data sovereignty risk management. In

---


6 Q2 2015 net sales of Amazon Web Services (AWS) were $1.824bn, up 81% year on year and 7.9% of total Q2 revenues of $23.2bn (available at http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-reportsother). For Microsoft, Q4 2015 commercial cloud revenue grew 88% to an annualised run rate of over $8bn, where $8bn would represent 8.5% of total FY 2015 revenues of $93.6bn (available at https://www.microsoft.com/investor/EarningsAndFinancials/Earnings/PressReleaseAndWebcast/FY15/Q4/default.aspx)


8 As of late August 2015, the most recent story is Ashley Madison, where hackers are reported to have taken customer details from publisher Avid Life Media’s systems (thought not to be in-cloud) on 15 July and posted them online by 18 August 2015.
the words of research firm Gartner from July 2014:⁹

“The number of data residency and data sovereignty discussions have soared in the past 12 months, stalling technology innovation in many organizations. Originally triggered by the dominance of US providers on the Internet and the Patriot Act, the perceived conflict was then fueled by revelations of unexpected surveillance by the National Security Agency (NSA) made public by Edward Snowden.

IT leaders find themselves entangled in data residency discussions on different levels and with various stakeholders such as legal advisors, customers, regulatory authorities, employee representatives, business management, and the public.

Business leaders must make the decision and accept the residual risk, balancing different types of risk: ongoing legal uncertainty, fines or public outrage, employee dissatisfaction or losing market share due to a lack of innovation, or overspending on redundant or outdated IT.”

5. **Aims and scope of this white paper.** This paper reviews cloud data sovereignty from the perspective of the practical steps that businesses may consider in order to mitigate the risks of adverse action that they and their customers may face, and the legal background that provides the context for those practical steps. The area is fast moving and **Section B** overviews various strands of data sovereignty in the news. **Section C** provides a concise legal background to data sovereignty legal issues in the area of investigatory powers. **Section D** isolates specific data sovereignty issues that arise in the cloud and suggests practical risk management steps that may be taken to address them from the perspectives of the Cloud SP and the CSC. Although a number of later developments have been tracked, the paper is written as at 1st September 2015 and from the perspective of English law, making reference where relevant to the laws of other countries.

**B. DATA SOVEREIGNTY IN THE NEWS**

6. **Introduction.** Issues touching on data sovereignty have been much in the news since mid-2013. This section reviews the legal background to the main stories – the Snowden allegations about bulk information collection programmes said to be carried out by the USA (paragraph **B.7** below); Mr Max Schrems’ litigation against Facebook (**B.8** below); Microsoft’s litigation over the warrant to obtain information for US proceedings from its Dublin data centre (**B.9**); the UK High Court effectively striking down s1 DRIPA on 17 July 2015 (**B.10**); and the three UK 2015 reviews into electronic surveillance of communications content and other data (**B.11**). All five stories share a number of common data sovereignty characteristics:

- the rights of citizens to privacy and protection of their personal data;
- the powers of the state to obtain, collect and use electronic communications information generated by their citizens without their agreement or knowledge;
- the appropriate balance between these citizens’ rights and state’s powers; and

---

in the international context, how these rights and powers play out if one state collects or obtains data not about its own, but about another state’s, citizens.

7. **The Snowden allegations.** In June 2013, following unauthorised disclosures by Edward Snowden, who had unlawfully taken papers from the US National Security Agency (NSA) whilst a NSA contractor, the Guardian and Washington Post newspapers published allegations\(^\text{10}\) about bulk information collection programmes said to be carried out in the USA by the NSA and also in the UK by the Government Communications Headquarters (GCHQ).\(^\text{11}\) Except for the PRISM programme, the UK Government has assumed a strict policy of ‘neither confirm nor deny’.

The programmes were said to be authorised in the USA under s215 Patriot Act 2001\(^\text{12}\) and s702 Foreign Intelligence Surveillance Act 1978, as amended (FISA). The Patriot Act programme is reported to authorise bulk collection of domestic US telephone call metadata (i.e. call records but not call content as ‘data about data’). Under the FISA programmes, the NSA is said to collect the content of emails and calls where the target is reasonably believed to be a non-US national located outside the USA.

Media attention has focused on ‘PRISM’ collection\(^\text{13}\), a s702 FISA programme operated by the NSA under the authority of the US Attorney General and Director of National Intelligence by which it is said that nine US internet companies\(^\text{14}\) are compelled to provide to the NSA directly from their servers data extending beyond metadata to include email, chat, videos and video conferencing, photos, stored data, VOIP (but not other telephone) calls and social networking details. The NSA is reported to share PRISM data with the US Federal Bureau of Investigation (FBI), the US Central Intelligence Agency (CIA) and the UK’s GCHQ.

A second s702 FISA collection programme is said to be ‘UPSTREAM’ and to involve compelled assistance from communication service providers (Comms SPs)\(^\text{15}\) as the operators of the

---


\(^\text{11}\) Mr Snowden was the subject of a BBC Panorama television programme, ‘Edward Snowden: Spies and the law’ transmitted on 5 October 2015.

\(^\text{12}\) In June 2015, the USA Freedom Act restored in modified form a number of provisions of s215 Patriot Act which had just expired. The modifications include limitations on bulk collection by US intelligence agencies of communications data relating to US citizens.


\(^\text{14}\) Said to be AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo and YouTube.

\(^\text{15}\) Traditionally, Comms SPs (or CSPs) are fixed telecommunications infrastructure operators (like incumbent telcos who trace their origins back to state owned PTTs) and mobile network operators (MNOs) who provide mobile network connections, each under contract to their customers. The distinction between fixed and mobile providers continues to erode. Internet Service Providers (or ISPs) historically provide access or connection to the internet to their contract customers. ISPs can include Comms SPs and specialist providers. The
telecommunications backbone over which messages are communicated, upstream of the PRISM internet companies.

‘TEMPORA’ is said to be the name of a programme operated by GCHQ to intercept data transmitted over underwater fibre optic cables landing in the UK, where between 10% and 25% of global telecoms and internet is estimated to transit the country via these cables, the data collected is similar to that provided under PRISM and there were allegedly to be 46 cables (out of an estimated global total of 100,000 bearers) tapped in this way in 2012.\textsuperscript{16}

Disclosure of the PRISM programme has caused international consternation with attention centring on its legal basis; the impact of the unauthorised and unlawful disclosures on the security services concerned; the appropriate legal balance between citizens’ personal freedoms and the responsibility of the state to ensure citizens’ safety; and the way forward at a time of perceived increasing threat from terrorism. A particular focus has been on the collection of data from outside the USA and a perceived diminution of data sovereignty for the countries concerned. Especially within the within the EU, this has centred on EU data protection rules. For example, in its statement responding to US law enforcement agencies’ access to personal data at the time of the Snowden revelations, a spokesperson from the UK Information Commissioner’s Office (ICO) said\textsuperscript{17}:

“There are real issues about the extent to which US law enforcement agencies can access personal data of UK and other European citizens. Aspects of US law under which companies can be compelled to provide information to US agencies potentially conflict with European data protection law, including the UK’s own Data Protection Act. The ICO has raised this with its European counterparts, and the issue is being considered by the European Commission, who are in discussions with the US Government.”

8. \textbf{Schrems v Facebook}. The Max Schrems case also highlights the nexus between the security of personal data in the Cloud, rights to privacy, data transfers from the EU to the USA and data sovereignty. Mr Schrems, then a law student at the University of Vienna, made a subject access request under Ireland’s Data Protection Acts 1998 and 2003 to Facebook’s Ireland subsidiary (FB-I) as data processor for the personal data it held about him. In response he received from FB-I a PDF file containing 1,200 pages. On reviewing the data, Mr Schrems on 18 August and 19 September 2011 made twenty-two formal complaints to the Office of the Irish Data Protection Commissioner (IDPC) about the way in which his personal data was held and handled by FB-I.\textsuperscript{18} The IDPC carried out an audit of FB-I, publishing its report in December 2011. The report contained

devlopement of the internet and (particularly mobile apps) has led to the development of ‘Over the Top’ (OTT) providers who supply their service ‘over the top’ of, and without necessarily billing their customers for, network connection. The terms Comms SP, ISP and OTT are increasingly fluid as a provider organisation may have functions of each. For example, the US internet providers mentioned in relation to PRISM may or may not be ISPs in the traditional sense of providing contract internet access or connections and may or may not be OTTs, and many Comms SPs/ISPs are combining with OTT providers. Finally, Cloud SP and Comms SP are used to distinguish the provision of cloud computing services defined at paragraph A.2 and telecommunications services described in this footnote. With these reservations, the terms are used in this sense in this white paper.

\textsuperscript{16} See IRTL Report (see paragraph B.11 below) Annex 7, paragraph 5, p. 330 and paragraph 4.13, p. 51.


\textsuperscript{18} See http://europe-v-facebook.org/EN/Complaints/complaints.html for the complaints.
a list of detailed, time-lined best practice recommendations for FB-I and provided for a formal review in July 2012 about the recommendations’ implementation. The review was duly reported on by the IDPC in September 2012. The second report noted FB-I’s ‘constructive approach’ and that ‘most of the recommendations have been fully implemented to our satisfaction’. Mr Schrems responded to the IDPC report that ‘the audit has led to many steps in the right direction but was unable to solve any of the complaints’.

Following the Snowden revelations in June 2013, Mr Schrems on 25 June 2013 filed a further complaint with the IDPC against FB-I about Facebook’s compliance with EU data protection law in the context of the operation of the EU/US safe harbour regime and Facebook’s alleged participation in the then newly revealed PRISM programme. Facebook and the other companies concerned had each registered under the safe harbour regime established by agreement between the EU Commission and the US Department of Commerce of 26 July 2000 and held by Commission Decision (the ‘Safe Harbor Decision’) to permit transfers of personal data from the EU to the USA compliantly with Article 29 of the EU Data Protection Directive. The basis of Mr Schrems’ complaint was that use of that data for the purposes of the PRISM programme would be unlawful under EU data protection law and also violate his rights to the protection of personal data under Article 8(1) of each of the European Convention on Human Rights (ECHR) and Charter of Fundamental Rights of the European Union (EU Charter).

The IDPC by letter on 23 July 2013 decided not to investigate the complaint against FB-I on the grounds that it was frivolous or vexatious under the Irish law. Mr Schrems (who had also instituted a class action) applied on 24 October 2013 in the Irish High Court for judicial review of the IDPC’s decision. In his judgment of 18 June 2014, Justice Hogan confirmed that the IDPC was bound to follow the EU’s finding in July 2000 that the Safe Harbor Decision complied with EU law. However, at paragraph 84 of the judgment, he referred the case to the Court of Justice of the European Union (CJEU) because of the critical issue that arose:

19 http://www.dataprotection.ie/docs/21-09-12-Facebook-Ireland-Audit-Review-Report/1232.htm
20 Mr Schrems also on 25 and 26 June 2013 filed complaints against each of Apple (to the IDPC), Microsoft and Skype (to the Luxembourg data protection regulator) and Yahoo (to the Bavarian data protection regulator) – see http://www.europe-v-facebook.org/EN/Complaints/PRISM/prism.html. To date, there has been little progress on the Luxembourg and Bavarian complaints.
25 See https://www.fbclaim.com/ui/page/faqs#klage
"whether the proper interpretation of the 1995 Directive and the [Safe Harbor] Decision should be re-evaluated in the light of the subsequent entry into force of Article 8 of the [EU] Charter and, whether as a consequence, the [IDPC] can look beyond or otherwise disregard the [EU] finding."27

The matter having been referred to the CJEU as Case C-362/14, the Oral Hearing took place in Luxembourg on 24 March 2015. The Advocate-General, Mr Bot, was due to deliver his opinion on 24 June 2015, but the date was postponed, it was thought, in view of ongoing discussions between the EU and the USA over updating the safe harbour regime28. The opinion29 was delivered on 23 September 2015 and found that the existence of a Commission Decision that a third country ensured an adequate level of protection of personal data transferred could not eliminate or reduce national data protection regulators’ powers under the Data Protection Directive and that the national regulators were free to suspend transfers which they considered were not compliant with Article 29 of the Directive.

In an important decision that has attracted widespread media coverage and legal interest, the CJEU gave judgment on 6 October 201530:

• confirming A-G Bot’s opinion that a Commission Decision as to the adequacy of third country data protection could not affect national regulators’ powers;
• holding that national regulators must be free independently to assess whether or not the transfer of a person’s data to outside the EU complies with the Data Protection Directive’s requirements, if need be applying to their own national courts for the question to be referred to the CJEU, which would thus ultimately decide on validity of the Commission Decision concerned;
• declaring the Safe Harbor Decision invalid as non-compliant with the EU Charter’s fundamental rights and freedoms first, because US authorities were bound to comply with US law as to data collection in disregard of safe harbour protection in circumstances where US law, in generally authorising storage of all personal data concerned without ‘differentiation, limitation or exception’ went beyond what was strictly necessary; second, because it did not provide for individual legal redress for data access, rectification or erasure; and third, because the Commission did not have power to restrict national regulators’ powers in the way the Safe Harbor Decision purported.

Consequently the referring the Irish High Court must examine Mr Schrem’s and, in the words of the CJEU press release31:

27 Paragraph 84
28 In the 2015 EC Management Plans published on 24 August 2015, the adoption of an EU-US Data Protection Umbrella Agreement and a Safe Harbor review were listed as among the main data protection outputs for 2015 of the DG Justice & Consumer Affairs, along with the adoption of the proposed general Data Protection Regulation (DG JUST Mgt Plan32, http://ec.europa.eu/atwork/synthesis/amp/index_en.htm). Discussions on the agreement were reported as finalised on 8 September 2015 although the Commission stated that the agreement could not be finalised until the right for EU citizens to judicial redress had become enshrined in US law.
“decide whether, pursuant to the directive, transfer of the data of Facebook’s European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data”.

The Irish Data Protection Commissioner has indicated that she will follow up the case in the Irish courts. The judgment will have also broader implications for the companies said to be involved in PRISM (see paragraph B.7 above); for the EU-US Data Protection Umbrella Agreement (see footnote 28) and wider EU-US trade relations generally; for the upcoming review of the UK’s surveillance laws (B.11 below); for the trend to national data retention laws (C.17); and for the progress of the draft General Data Protection Regulation (C.21). Although the case starkly points up the tension between citizens’ rights and the state’s powers and it is likely in the short term to increase friction in digital business, it remains to be seen what, if any, long term impact it will have.

9. **Microsoft v United States: In re Warrant etc.** In December 2013, US federal prosecutors during the course of a narcotics criminal investigation obtained from a federal Magistrate in New York an authorisation under the US Stored Communications Act 1986 (SCA) for the search and seizure of information including emails associated with a Hotmail account stored by Microsoft at its data centre in Dublin, Ireland. Microsoft unsuccessfully challenged the warrant before the issuing New York Magistrate and then appealed before the federal US district judge, who on 29 August 2014 held for the Magistrate and removed the suspension of the authorisation.\(^{32}\) Microsoft then on 5 September 2014 requested of its own volition that it be held in contempt of court for failure to comply, opening the way to appealing the district judge’s decision to the US Court of Appeals.

The case is significant as the first time that data sovereignty issues have been litigated about the production in one country’s domestic proceedings of electronic data stored in another country. The significance is heightened by the growth of Cloud services, the perceived intrusiveness of US state surveillance after Snowden and general security concerns about private data stored in the cloud.

The legal arguments in the case are fairly specific and turn on the interpretation of US legislation passed in 1986, before widespread adoption the internet, email and the cloud. The central issue is whether the nature of the hybrid authorisation under the SCA prevails as a subpoena (requiring production of information regardless of location in the ‘possession, custody or control’ of a recipient who is subject to the court’s personal jurisdiction) or a warrant (which is subject to much stricter territorial jurisdictional constraints). The United States contends that the SCA authorisation is a subpoena with which Microsoft, as a legal entity within the personal jurisdiction of the US court, is bound to comply. Microsoft argues that under US law the SCA authorisation is a warrant and so, under US criminal procedure rules, does not extend to outside the USA.

The case has attracted attention. On 6 June 2014, Mr Michael McDowell, a former Attorney General of Ireland, made a declaration in the proceedings that if Microsoft complied with the SCA authorisation it would be in breach of Irish law if the disclosure was not subject to control by the Irish courts. On 15 December 2014, Cloud SPs including Amazon, Apple, Cisco, eBay, Hewlett-Packard, Salesforce and Verizon all filed amicus curiae briefs in support of Microsoft. On 23 December 2014, 

\(^{32}\) *In re Warrant to search a Certain Email Account Controlled & Maintained by Microsoft Corp* 15 F. Supp. 3d 466 (S.D.N.Y. 2014). For a timeline of the case and compendium of materials, see [http://digitalconstitution.com/about-the-case/](http://digitalconstitution.com/about-the-case/)
the Government of Ireland filed a further *amicus curiae* brief asserting both that the US court was required to respect Irish sovereignty, and its willingness to consider a request under the US/Ireland Mutual Legal Assistance Treaty ‘should one be made’ as an alternative way to disclose the information sought. Oral hearings in the case took place on 9 September 2015, when the US Court of Appeals heard the US Government. Judgment is expected within the next few months.

10. **The UK Data Retention and Investigatory Powers Act 2014 (DRIPA).** On 17 July 2015, following a challenge by Members of Parliament David Davis and Tom Watson, the UK High Court decided that s1 DRIPA was unlawful, or more particularly that the provision was incompatible with the judgment of the CJEU in case C-293/12 (*Digital Rights Ireland Ltd*). In *Digital Rights Ireland* the CJEU had to consider whether the EU Data Retention Directive 2006/24 was compatible with Articles 7 and 8 of the EU Charter. The directive provided for each EU Member State (MS) to require Comms SPs and ISPs to retain for between six and twenty-four months certain categories of communications data (broadly, message metadata including date, time, duration, subscriber ID, caller ID, receiver ID, etc., but not the content of the message itself). Articles 7 and 8 of the EU Charter enshrine the fundamental principles of respect for private and family life and protection of personal data. The CJEU concluded (at paragraph 69 of the judgment) that ‘by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7 [and] 8 of the [EU] Charter’, effectively striking down the directive.

The UK Government had enacted Directive 2006/25 in two statutory instruments (the UK’s main form of delegated legislation), one for fixed network and mobile telephony (broadly, Comms SPs) and the other for internet access, telephony and email (broadly, ISPs and certain OTTs). It now had an uncomfortable legislative gap to fill in order to empower the UK intelligence Agencies (MI5, MI6 and GCHQ), police and other public authorities to continue collecting and using communications data and hurried the DRIP Bill through all stages of Parliament in four days. DRIPA received the Royal Assent and came into force on 17 July 2014. S1 DRIPA was the replacement provision for

the regulations struck down in Digital Rights Ireland. The Act included, at s8(3), a ‘sunset clause’ timing it out on 31 December 2016.

DRIPA had been widely criticised for the speed with which it was introduced; the breadth of the powers granted; and the lack of debate about its scope and detail. The two Members of Parliament and a number of civil liberties groups applied for judicial review. The case was heard on 4 and 5 June and 9 July 2015. Judgment was given on 17 July, when the High Court allowed the application, ordering that s1 DRIPA be disapplied on the grounds that it was incompatible with EU law as it failed the proportionality test regarding Articles 7 and 8 of the EU Charter in the same way as had the Data Retention Directive in Digital Rights Ireland. The court gave leave for the Government to appeal and delayed the order until 31 March 2016, effectively bringing forward DRIPA’s sunset by nine months and the debate about the replacement legislation to the 2015/16 session of Parliament.

11. Upcoming review of UK telecoms and internet surveillance laws. As if to pave the way for this debate, three reports have been published in 2015 on the UK regime of investigatory powers, each focusing on electronic surveillance.

First, on 12 March 2015 the Intelligence and Security Committee of Parliament (ISC) published ‘Privacy and Security: a modern and transparent legal framework’, billed as the first time that a single document had ‘provided a comprehensive review of the full range of intrusive capabilities available to the UK intelligence Agencies’.

Second, on 6 May 2015 pursuant to s7 DRIPA David Anderson QC, the UK’s Independent Reviewer of Terrorism Legislation (IRTL), sent to the Prime Minister his 300 page review of UK law governing the use of communications data and interception, ‘A Question of Trust – Report of the Investigatory Powers Review’ (the IRTL Report). His report was published on 11 June 2015. In seeking to inform the parliamentary and public debate, it clearly and comprehensively reviews relevant legal, technological and operational aspects as well as the views of government agencies, the service provider community and civil society as the main stakeholders. The IRTL Report then articulates 124 recommendations for reform and the principles underlying them, in turn building on five guiding principles of minimising no-go areas for law enforcement; limiting powers in the interests of privacy; respect by the state for guaranteed rights and freedoms; legislative clarity and transparency; and a unified legislative approach.

Third, on 14 July 2015 the Independent Surveillance Review (which had been commissioned in March 2014 by the then Deputy Prime Minister to review UK surveillance programmes in the wake of the Snowden allegations) published its report ‘A Democratic Licence to Operate’ under the auspices of the Royal United Services Institute (RUSI).

Each of the ISC, IRTL and RUSI reports recommends an overhaul of the UK’s legislation.

40 http://isc.independent.gov.uk/committee-reports/special-reports
41 https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/#more-2364
C. DATA SOVEREIGNTY: LEGAL BACKGROUND

12. **Data sovereignty and the state's investigatory powers: introduction.** As business and individuals’ data migrate to the cloud, commercial and consumer concerns about loss of sovereignty over their customers’ or their own data, heightened by new stories of the type described at Section B, are at their most acute in relation to the perceived extent of the state’s investigatory powers to obtain their cloud data. In fact, and as we will see in Section D below, the differences between the state’s powers over data communicated electronically held on-premise (on the one hand) and in-cloud (on the other) are less than might first be imagined. The same is also true when considering those powers as they exist in different countries throughout the world. This is not because countries’ powers to intercept and collect in-cloud over and above on-premise data are insubstantial but rather because their powers to intercept and collect data from all electronic communications are so broad.

A detailed discussion of the UK law of investigatory powers about interception and communications data is outside the scope of this paper. However, a concise overview is helpful to set the context for how on-premise and in-cloud data sovereignty issues differ and the practical steps businesses may take to address cloud data sovereignty risks (Section D). Accordingly, this section considers first the state’s powers (C.13 – C.19 below) and then citizens’ rights (C.20 and C.21). Paragraph C.13 summarises the framework of investigatory powers under UK law. C.14 focuses on the UK government’s powers under RIPA. Extra-territorial reach of interception and collection laws in the UK (C.15) and other countries (C.16) is then briefly considered, followed by a quick look at the trend towards national data residency, localisation or domiciliation laws (C.17), mutual legal assistance treaties (MLATs) (C.18) and treatment of legal professional privilege (LPP) and related issues (C.19). As to citizens’ rights, in the absence of protection at common law for the privacy of communications (C.20), the extent to which legislation protecting basic individual rights and freedoms (including respect for private and family life and protection of personal data) may override the existence or exercise of the state’s powers is briefly considered at C.21.43

**The State’s Powers**

13. **The framework of investigatory powers under UK law.** The law of search and seizure has always been bound up with technological and commercial developments and the constant tension between ‘extensive executive action in the interest of public order’ and ‘strict procedural safeguards’ on that action44, most classically in relation to the UK 1760s cases on publishing and general warrants of arrest and for search and seizure of property. In the area of communications, the tension is fundamentally the same, with the emphasis on intangible information rather than the person and tangible property. Up to 1981 telecommunications and interception both operated in the UK behind the veil of the state as the provision of telecommunications services was the monopoly of the state-owned General Post Office. Since then, telecommunications has been progressively and extensively

---

43 For a thorough and comprehensive review of current legal powers, safeguards and constraints about UK government agency investigatory powers, see Part II, Chapters 5 and 6 (pages 71 to 123) of the IRTL Report.
44 For an excellent summary of the historical background see in particular Polyvios G Polyviou, *Search and Seizure*, (1982, Duckworth) Chapters 1 and 2. The quotations are from page 5.
liberalised and deregulated\(^{45}\), the UK intelligence Agencies have been formally avowed and put on a statutory footing\(^{46}\) and communications interception has been made subject to legislation.\(^ {47}\)

The start point for the UK investigatory powers law analysis is that intercepting communications or gathering information about telecommunications service use is unlawful under UK law unless either the user’s consent has been obtained\(^ {48}\), it is in exercise of a warrant or statutory power properly conferred or it is otherwise authorised.\(^ {49}\) The enabling UK statutory framework is complex:

- at its centre sit the powers to intercept and to obtain communications data under the Regulation of Investigatory Powers Act (\textit{RIPA})\(^ {50}\);
- powers to intercept wireless communications are also conferred under ss48 and 49 WTA\(^ {51}\) with further broad powers provided for by s94 BTA\(^ {52}\);
- specific public authorities have numerous other powers to gather data\(^ {53}\); and
- UK intelligence services have other specific powers of surveillance, interference and intrusion under the SSA and the ISA.

As we have seen at paragraphs B.10 and B.11, UK law in this area generally and RIPA in particular is in a state of flux. The IRTL Report stated in its summary of proposals for reform (page 5, paragraph 14):

“RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of

\(^{45}\) The British Telecommunications Act 1981 transferred the UK telecommunications network from the GPO to a new statutory corporation, British Telecommunications (BT) as a monopoly provider but with power for the Government to license others. The British Telecommunications Act 1984 (BTA) provided for the privatisation of BT; the establishment of OFTEL as the UK telecommunications regulator; and the introduction of a licensing system for fixed line telecommunications systems and services, and interconnection between them. The BTA was superseded by the Communications Act 2003, the current statute, which consolidated and overhauled the UK framework for telecommunications and broadcasting; replaced OFTEL and the previously separate radio and broadcasting regulators with Ofcom; and substantially liberalised and deregulated the provision of UK telecommunications and broadcasting. Broadcasting, radio spectrum and wireless telegraphy (as opposed to fixed line telecommunications) were subject to a separate licensing regime under wireless telegraphy legislation from the early 1900s (notably the Wireless Telegraphy Act 1949 under which the first UK mobile licences were granted) which was consolidated and updated into the Wireless Telegraphy Act 2006 (WTA).


\(^{48}\) S1(1) and (3) RIPA; ss48(1) and (3) WTA.


\(^{53}\) See IRTL Report, Annex 6, List of Bodies with non-RIPA powers, pages 323 to 330).
them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and - in the long run - intolerable.”

14. The framework of UK data interception and collection law: RIPA and DRIPA. RIPA’s core concepts are the definitions of and distinctions between interception and communications data and the ways in which powers for each may be applied for, authorised and used. Added to this may be added the ‘home and away’ distinction between in-country and external communications.

Interception

By s2 RIPA, interception is the monitoring or collecting of the ‘content’ of a communication ‘in the course of transmission’. ‘Content’ is not defined (as distinct from communications data, which is) but includes everything to do with the communication and its related communications data (as defined at s20): broadly, content is the message along with its associated metadata as the envelope. Importantly, under s2(7), ‘in course of transmission’ includes any time when the communication is stored so that the intended recipient can access it. Interception therefore does not have to be ‘live’ - as the message is being sent - but can take place at any time after it has been sent so long as it is retrievable by the recipient.

Communications data

Communications data exclude the content of the communication and by 20(4) RIPA cover three types of data about the use made of the service relating to the communication, service or subscriber concerned: traffic data (envelope); service use data (e.g. itemised phone bill); and subscriber data (including details provided to the service provider). Communications data do not have to be obtained ‘in course of transmission’ (as do interceptions) but are obtained afterwards from the service provider.

Interception powers

RIPA interception powers can only be applied for by a limited number of specified services, and are authorised and exercised by means of warrant under ss5 and 8, which must be signed by a Secretary of State or Scottish Minister on their belief that the warrant is necessary on grounds of national security, combatting serious crime, safeguarding the UK’s economic well-being or to give effect to an international agreement (s5(3)). Under s8(1) interception warrants may be either targeted to a single person or set of premises or themed to an organisation or group of persons. S8(1) warrants may authorise the interception of communications between two people in the British Islands (in the language of RIPA) or overseas. Bulk (or external) warrants issued under s8(4) authorise interceptions where the communication sender(s) or recipient(s) are outside the British Islands. Bulk warrants may be used for interception of all communications carried over a specified route or cable or by a specified service provider.

54 MI5, MI6, GCHQ, the National Crime Agency, the Metropolitan, Northern Ireland and Scottish police services, Her Majesty’s Revenue and Customs and the Ministry of Defence.

55 IRTL Report, paragraph 6.43 page 106. See also paragraph B.7 above in relation to TEMPORA.
Communications data powers

The basis on which service providers are required to hold (for up to a year) communications data is currently a notice from the Home Secretary under s1 DRIPA. As we have seen at B.10 above, the relevant powers under s1 DRIPA, hurried through Parliament in July 2014 to replace the previous rules declared unlawful under Digital Rights Ireland, were themselves disappplied by the High Court on 17 July 2015 on a delayed basis until 31 March 2016 for the same reasons as the previous rules.

UK public authorities may apply for authorisation to obtain access to communications data as set out in ss21 to 25 RIPA. Access conditions are less restrictive than for interception: many more authorities (about 600) can apply to obtain access; the application can be on broader grounds; authorisation may be granted by many more designated persons; and the authorisation simply has to describe the data required.

Guidance in the form of codes of practice concerning use of RIPA powers for both interception and obtaining communications data, including as to the safeguards for their use, is published by the Secretary of State56.

‘Home and away’

According to the IRTL Report (paragraph 5.36, page 79) most if not all countries’ legislation distinguishes between ‘internal’ or ‘domestic’ communications and the protection given to a country’s nationals (on the one hand) and ‘external’ or ‘foreign’ communications and protections for non-nationals (on the other). In the UK under RIPA, whilst the boundary between s8(1) targeted or themed warrants and s8(4) bulk or external warrants is relatively clear, the boundary between internal and external communications is less clear, giving rise to increasing interpretation difficulties in a world where global services are growing fast.

15. The extra-territorial reach of UK data interception and collection law. The convergence of the cloud, mobile, social media and big data is driving both a vast increase in data volumes and the globalisation of that data. At the same time, the development of the internet (and particularly mobile apps)57 has led to the fragmentation of communications-related services, with many kinds of service provision all producing content and communications data, and many kinds of Comms SP, ISP and OTT58 who may be located almost anywhere in the world. This combination of service provision globalisation and fragmentation has gone hand in hand with rapid development in encryption, anonymity and anti-surveillance techniques. All this poses (in the words of the IRTL Report at paragraph 6.95, page 118) ‘unique jurisdictional challenges when UK law enforcement agencies wish to gain access to […] data [in the possession of overseas service providers]’. This is the context for s4 DRIPA, which sought to clarify the provisions of RIPA dealing with extraterritorial application.

56 See https://www.gov.uk/government/collections/ripa-codes

57 Small (in terms of code size) pieces of application software that reside on a smartphone, tablet or other mobile device as a front end that enable the device user to access the app provider’s service.

58 See footnote 14 for an explanation of these terms and how they are used in this white paper.
Interception

As regards interception, a person (the service provider concerned) is required under s11 RIPA as amended by s4 DRIPA to give effect to an interception warrant served on them whether or not they are in the UK, except for steps it is not reasonably practicable for them to take (taking into account the law of the country where they reside), and risks committing an offence for knowingly failing to comply. By s12 RIPA as amended, the Secretary of State may require anyone providing public telecommunications services (broadly defined) whether or not they are in the UK to provide assistance regarding an interception warrant.

Communications data

For communications data, the access requirement may relate to conduct, and be imposed on a person, outside the UK and the service provider must comply with the requirement irrespective of the operator’s location provided it is reasonably practicable.

In the words of the IRTL report (paragraph 6.99, page 118):

“Whether or not the UK Government could enforce these obligations in relation to service providers has not yet been tested and there remain some overseas service providers who do not consider they are bound by RIPA. As a matter of practice, such cooperation as is forthcoming from overseas [service providers] comes from informal requests for assistance.”

16. Extra-territorial reach: other countries’ laws. The same problem of extra-territorial reach that s4 DRIPA, ostensibly confirming RIPA, has sought to solve in the UK arises for other countries and should properly be seen as one of the broader contexts for the Snowden revelations overviewed at B.7 above. The IRTL Report at paragraph 5.36 (page 79), paragraph 8.41 (page 148) and Annex 15 (pages 349 to 368) summarises the equivalent rules to those overviewed at C.13 to C.15 above in Australia, Canada, New Zealand and the United States, the other countries along with the UK in the ‘Five Eyes Partnership’ of those countries’ security and intelligence agencies.

Annex 15 notes:

- **Australia**: the Australian Telecommunications (Interception and Access) Act 1979 envisages the interception of ‘foreign intelligence’ and access to foreign stored communications;

- **Canada**: Canadian law provides for interception of private communications originating or intended to be received in Canada (Protection of Privacy Act 1974) and a separate regime for security service access to ‘foreign intelligence’ (Canadian Security and Intelligence Services Act 1984);

- **New Zealand**: the New Zealand Security Services Intelligence Act 1979 provides for warrants to intercept foreign intelligence and communications sent from or to an overseas country; and

- **USA**: FISA in the USA governs the collection and analysis of foreign intelligence and authorises the electronic surveillance of foreign powers overseas, including international terrorist groups, agents of foreign powers and the activities of non-US citizens within the USA. FISA authorises three kinds of data collection: first, by a Federal officer with the approval of the Attorney General and under a warrant issued by the special FISC court; secondly (and as we have seen at B.7) by the Attorney General and Director of National Security under the s 702 FISA; and thirdly under
the process known as s215 by the Director of the FBI. An important distinction between UK and US law that service providers in the USA are not required to store data beyond their own business needs (such as billing data) or what they already produce and create.

In the wake of Digital Rights Ireland (B.10), many EU countries are reviewing their own laws. For example, in the Netherlands the Dutch Data Retention Law was declared unlawful by the District Court of The Hague in March 2015; and following the Charlie Hebdo murders in Paris in January 2015, France introduced in March 2015 a new Intelligence Bill which was approved by the French Conseil Constitutionnel on 23 July 2015. However, the Conseil Constitutionnel did intervene to strike out the proposed article of the new Bill dealing with interception and control of communications sent or received outside France on the grounds that it did not specify conditions for authorisation, or preserving or destroying information collected under it.

17. A trend towards data residency, localisation and domiciliation laws? At the same time as communications in one country may be subject to interception and surveillance by another, the position is further complicated by a nascent trend towards national residency, localisation or domiciliation laws to enforce the retention of data in the country of origination. In Russia, Federal law No. 242-FZ of 21 July 2014, which came into force on 1 September 2015, requires operators using servers to collect, aggregate, store, update and extract personal data of Russian citizens to locate those servers in Russia. The law has raised many questions, particularly:

- **retrospective effect**: it is believed that only personal data collected after 1 September 2015 will require to be processed in compliance with the law but that this will include pre-September 2015 data as soon as it is collected, stored, updated or extracted;

- **transition**: it is believed that large non-Russian internet companies will have until 2016 to comply; and

- **transfer of such data to outside Russia** and extra-territorial reach.

Roskomnadzor, the Russian data protection regulator, has held a number of meetings over summer 2015 to seek to resolve these questions. China and Vietnam have also passed data localisation laws.

18. Mutual Legal Assistance Treaties (MLATs). The MLAT system is an established network of bi- and multi-lateral agreements between countries used by law enforcement for international assistance in gathering and exchanging information for criminal investigations and prosecutions. Although extending to electronic communications, the agreements concerned generally pre-date the cloud, if not the internet and email, and the procedures they establish are too slow to be effective.

---

59 See also footnote 11 above on the impact of the USA Freedom Act on s215.
60 The draft Bill as introduced to the French Senate is at [http://www.senat.fr/leg/pjl14-424.html](http://www.senat.fr/leg/pjl14-424.html)
63 See FT report at [http://www.ft.com/cms/s/0/e11024f4-e281-11e4-aa1d-00144feab7de.html#axzz3jij2RbxLa](http://www.ft.com/cms/s/0/e11024f4-e281-11e4-aa1d-00144feab7de.html#axzz3jij2RbxLa)
The US December 2013 report ‘Liberty and Security in a Changing World’ commented at page 227 that:

“The MLAT process creates a legal mechanism for non-US countries to obtain e-mail records, but the process today is too slow and cumbersome. Requests appear to average approximately 10 months to fulfill, with some requests taking considerably longer. Non-US governments seeking such records can face a frustrating delay in conducting legitimate investigations.”

A practical example of the limitations of the MLAT system is the Microsoft case (B.9), where prosecutors sought to instruct Microsoft to produce information from the email account concerned through a US warrant instead of an MLAT request to the Irish authorities. In this case and as we have seen, the Irish Government also noted its willingness to consider an MLAT request ‘should one be made’ in the context of observations about the US court being required to accept Irish sovereignty.

MLAT overhaul is on the reform agenda. The December 2013 US report cited above recommends (at pages 226 – 228) streamlining the MLAT process ‘both in order to respond more promptly to legitimate foreign requests and to demonstrate the US commitment to a well-functioning Internet that meets the goals of the international community’ by increasing US resources allocated to MLAT requests, creating an online MLAT submission form and streamlining inbound and outbound processes. Similarly, the IRTL Report at Recommendation 24(c) (page 289) suggested that:

“in order to address deficiencies in access to material from overseas service providers, the Government should …

(b) seek the improvement and abbreviation of MLAT procedures, in particular with the US Department of Justice and the Irish authorities; and

(c) take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations.”

19. **Legal Professional Privilege (LPP), etc.** RIPA itself does not deal with information under LPP, journalistic information, medical records or other confidential information differently from other information, although the draft Interception Code and Acquisition Code published earlier in 2015 under RIPA referred to at footnote 51 now addresses this type of information. For example, under the draft Interception Code, an application for a warrant to intercept LPP information must satisfy the Secretary of State that there are ‘exceptional and compelling circumstances that make the warrant necessary’. Recommendation 67 the IRTL Report (Chapter 15, page 297) proposes:

“When the communications data sought relates to a person who is known to be a member of a profession that handles privileged or confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion), the new law should provide for the [Designated Person at the authority] to ensure that (1) special consideration is given to the possible consequences for the exercise of rights and freedoms, (2) appropriate arrangements are in place for the use of the data, and (3) the application is flagged for the attention of inspectors [of the Independent Surveillance and Intelligence Commission]).”

20. **Citizens’ Rights**

20. **No right to privacy at common law: non-applicability to communications of the 1760s warrant cases.** The ‘general warrant’ cases of the 1760s have been pleaded unsuccessfully in the UK in

---

65 See footnote 10
support of a common law rule for privacy of communications and against intrusion so that, as noted at paragraph 5.11 of the IRTL Report, ‘the perhaps surprising outcome is that the common law ... barely recognises the right to privacy or private communications’.

The general warrant cases of the 1760s were brought at a time of antipathy towards the new monarch George III and his executive that was articulated in pamphlets and coffee houses, the social media platforms of their time. In relation to broad warrants issued to search and seize the authors of offending material and their possessions, Pratt LCJ in *Wilkes v Wood*66 said:

“The defendants claimed a right, under precedents, to force persons’ houses ... seize their papers, etc. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders’ names are specified in the warrant, and therefore a discretionary power given to the messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject.”

Two years later in November 1765, Lord Camden LCJ (as Pratt LCJ had become a few months before) handed down the famous judgment in *Entick v Carrington*.67 Here, the facts were again that the Secretary of State had issued a general warrant, this time to Mr Carrington the King’s Messenger to search for Mr Entick, the author of a pamphlet libelling the King and Parliament, and ‘to seize and apprehend and bring together with his books and papers in safe custody ... to be examined concerning the premises, and further dealt with according to law’. Lord Camden LCJ held squarely that the general warrant was unlawful:

“our law holds the property of every man so sacred, that no man can set his foot upon his neighbour’s close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour’s ground, he must justify it by law... this is the first instance of an attempt to prove a modern practice of a private office to make and execute warrants to enter a man’s house, search for and take away all his books and papers in the first instance, to be law, which is not to be found in our books.”

Although the cases continue to be good law in the UK68 they have not led to a common law doctrine of privacy first, as they were brought in trespass and so grounded in the law of property and freedom of the person; and second, because UK courts69 since the advent of phone tapping have resisted applying them more broadly in favour of a common law communications privacy right, effectively saying this is a matter for Parliament.

A gloss on this it might be to suggest that, as intellectual property rights in relation to data continue to strengthen, interception, bulk collection and retention of data may raise questions of infringement of copyright, database right or confidence where the requisite grounds for subsistence of the right concerned and its infringement are made out.

68 And were influential in the USA in passing in 1791 the Fourth Amendment to the US Constitution (Amendment IV) prohibiting unreasonable searches and seizures and requiring warrants to be judicially sanctioned and supported by probable cause.
69 See e.g. *Malone v Commissioner of Police (No. 2)* [1979] 1 Ch 344 and more recently (in the Investigatory Powers Tribunal (IPT)) *Liberty & Ors v Secretary of State for FCA & Ors*, [2015] UKIPTrib 13_77-H
21. **Right to privacy, etc under the ECHR, EU Charter and data protection legislation.** In the absence of common law protection, it is therefore left to statute law to bear the weight of protecting basic individual rights and freedoms regarding privacy of communications. In the UK, outside the safeguarding provisions of RIPA and other relevant legislation, this protection is currently afforded by the EHCR as transposed into UK law by the Human Rights Act 1998\(^70\) (**HRA**), the EU Charter and applicable data protection law.

**The EHCR and HRA**

Since the HRA came fully into force on 2 October 2000, most of the ECHR’s ‘rights and fundamental freedoms’ have been enforceable as ‘Convention rights’ under the HRA in the UK courts, which must ‘take into account’ case law of the European Court of Human Rights (**ECtHR**) (s2(1)) and interpret UK legislation compatibly with the ECHR (s3(1)) and which may make a ‘declaration of incompatibility’ between the Convention rights and UK legislation (s4(2)). Relevant parts of the ECHR are Articles 6 (the right to a fair trial), 8 (the right to respect for private and family life, home and correspondence) and 10 (the right to freedom of expression). A number of cases are currently pending before the ECtHR concerning the compatibility of bulk data collection and data sharing practices alleged to be carried out by UK government Agencies with these ECHR rights and freedoms.

**The EU Charter**

The EU Charter came into effect on 1 December 2009 and has the same legal effect as the EU Treaties themselves so that EU legislative acts (decisions, regulations and directives) may be declared invalid by the CJEU and national Member State law must be disapplied by national courts in either case if inconsistent with the EU Charter. Articles 7 and 8 of the EU Charter protect the rights to respect for private and family life and the protection of personal data:

“The Article 7 - Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 - Protection of personal data.

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.”

It was inconsistency with Articles 7 and 8 that caused the CJEU to strike down the EU Data Retention Directive and the UK High Court to order the disapplication of s1 DRIPA with effect from 31 March 2016 (B.10).

Data protection legislation

The Data Protection Act 199871 (DPA, calling down into UK law the EU Data Protection Directive) and the Privacy and Electronic Communications (EU Directive) Regulations 200372 (the PECR, calling down the related EU directive73) set out the UK’s rules on the collection and processing of personally identifiable information relating to living individuals. Detailed consideration of the DPA and PECR are outside the scope of this paper. The DPA provides that, subject to certain exemptions (including for national security, crime and regulatory activity) personal data must be collected, processed and kept in accordance with eight data protection principles and must be accessible on request by the subject of the data concerned. ICO is the UK’s data protection regulator and its role is to ‘uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals’.74 Recital 2 of the Data Protection Directive ties it back to fundamental privacy rights:

“(2) Whereas data-processing systems … must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy …”

The PECR set out specific privacy rules on marketing calls, emails, texts and faxes and other electronic communications; data related to electronic communications including traffic and location data, itemised billing, line identification, and directory listings; cookies; and the security of communications services. Recital 2 of the Directive ties it back to the EU Charter:

“(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.”

The current EU data protection regime will be overhauled when the new General Data Protection Regulation comes into effect.75 As at end August 2015, the procedure towards the new regulation is in trilogue – informal, structured discussions between the EU Commission, Council and European Parliament – with a view to resolving all outstanding issues on the new rules by the end of 2015.

74 https://ico.org.uk/about-the-ico/
D. DATA SOVEREIGNTY AND CLOUD COMPUTING: SPECIFIC ISSUES AND PRACTICAL RISK MANAGEMENT

22. Data on-premise and in-cloud: isolating specific cloud computing data sovereignty issues. Compared with data processing in an organisation’s own server room or data centre, cloud computing involves three main additional steps: transit from the CSC’s own IT system to the Cloud SP; data processing and storage at the Cloud SP; and transit back to the CSC. This paper focuses on these cloud-specific data sovereignty issues rather than those that arise generally.

From Section C, it will be seen that whether or not an organisation uses the cloud, data in its own server room or data centre may potentially be subject to interception; the organisation’s communications (in common with organisations across the UK) are subject to bulk collection through the TEMPORA UK fibre optic cable interception programme (if the Snowden allegations are accurate in this respect); communications data of the organisation’s staff may be subject to law enforcement access through its service providers; and these interception and collection activities may be carried out by national and potentially by overseas agencies. Data sovereignty issues in the cloud therefore represent incremental risk rather than a completely new type of risk.

Equally, the distinction between on-premise and in-cloud processing and storage outside the investigatory powers arena is less relevant where the organisation’s processing or use of data (wherever held) is in breach of contract, third party intellectual property or other rights. Other potentially tortious or criminal activity like hacking, denial of service, malware or screen-scraping may engage an organisation’s data security, whether the data is held on-premise or in-cloud. Cloud data sovereignty risks, both as regards investigatory powers and as regards rights infringement and breach of duty more broadly, should therefore be seen on a continuum which includes on-premise and in-cloud.

The specific data sovereignty issues that arise for cloud computing differ when viewed from the perspective of the Cloud SP and the corporate and individual CSC. From the Cloud SP’s point of view (paragraph D.23 below), cloud data sovereignty issues centre around the extent to which it may be compelled by law to disclose a CSC’s data and by whom, and how this and related issues are dealt with by policy, contract and otherwise in relation to its organisational and individual customers. The point of view of the CSC (whether an organisation or individual) is primarily but not wholly contractual, from the other end of the telescope to the Cloud SP (D.24). For each, practical risk management steps are considered at D.26 to D.28.

23. Cloud SPs and data sovereignty issues. As mentioned above, Cloud SPs (as Comms SPs, ISPs and OTTs) operate in a world characterised by the globalisation and rapid evolution of big data and cloud computing. However, the current framework of investigatory powers law is based on national laws so that a Cloud SP operating internationally is subject to a wide and potentially inconsistent array of legal requirements. For a Cloud SP with international operations, this tension between ‘cloud as global, law as national’ can be articulated in the following layered way, where a given Cloud SP:

- is subject to intrusion (as government agency interception, communications data collection and other exercise of investigatory powers) in its home country (H) for its home country data centres under its home country (H) law [example: RIPA and a UK Cloud SP for its UK data centres];
may also be subject to certain home country (H) intrusion for data in any data centre under its control in any country (O) outside its home country (H) [example: Microsoft’s Dublin data centre and the US warrant at B.9];

is also subject to intrusion for data in any data centre outside its home country (H) under the law of the country where that data centre is located (O) and/or where the subsidiary operating that data centre is registered or otherwise located (R) [example: RIPA];

may also be subject to intrusion sought to be exercised by a government agency from any country (X) other than H, O or R under X’s laws for any data centre wherever located [example: RIPA/DRIPA extra-territoriality provisions];

in complying with the intrusion laws of an overseas country (O, R or X in any of the above examples), also risks breaching the home country’s (H) laws [examples: positions of FB-I at B.8 and Microsoft at B.9 where H is Ireland and O is the USA]; and

may be subject in one or more of these countries to specific residency, localisation or domiciliation requirements to for data originating in that country’s territory [example: Russia].

A further issue, particularly as regards the developing area of OTTs, is to determine which types of Cloud SPs are caught by the various investigatory powers nets.

Practically speaking, even though investigatory powers laws are currently being overhauled in many countries and streamlining of MLAT international cooperation is in prospect, it is reasonably foreseeable that such inconsistencies will not be completely ironed out in the short term. As new laws emerge, Cloud SPs will to an extent best be served by legal certainty in and between national laws (whatever the citizens’ rights aspects and from the shareholder perspective). Difficulties may arise for an international Cloud SP where its home country laws are unclear and give rise to conflicts with the law of another country in which it operates. Absent legal certainty, the scope of the contractual duties that a Cloud SP owes its customers may remain unclear, fuelling potential for disputes; and, in a particular fact situation, the Cloud SP may not easily be able to reconcile its conduct towards law enforcement agencies (to whom for any activity it may be under both compulsion and strong secrecy duties which may even forbid acknowledgement of the activity); customers and market perception (on which its reputation depends); and shareholders, again increasing the possibility of disputes.

These issues were addressed by service providers in their submissions to the IRTL and are summarised at Chapter 11 (pages 203 to 213) of the IRTL Report. In particular, Reform Government Surveillance (a group of US providers including all the companies said to be subject to PRISM compelled collection (see paragraph B.7) other than PalTalk together with Dropbox, Evernote, Linked in and Twitter) advocate the adoption of five principles76 which address:
• limiting government authority to collect users’ information;
• oversight and accountability;
• transparency about government demands;
• respecting the free flow of information; and

76 https://www.reformgovernmentsurveillance.com/
• avoiding conflicts among governments.

This complexity also explains why some Cloud SPs are offering contractual commitments as to data residency, localisation or domiciliation\(^{77}\) or restricting data storage to a particular country, region or geography\(^{78}\).

24. **CSCs and data sovereignty issues: contracting with the Cloud SP - investigatory powers, regulatory access, etc.** Data sovereignty issues for CSCs will generally arise in the framework of their contractual arrangements with their Cloud SP and, for CSCs supplying cloud-based services to their own customers, those CSC/customer agreements.

**Investigatory powers: the CSC/Cloud SP contractual context**

Treatment of CSC data in relation to the exercise of investigatory powers vis à vis the Cloud SP is as yet relatively undeveloped in Cloud SP/CSC contracting. This is an area where increased underlying legal certainty at the primary government agency/Cloud SP level will enable the Cloud SP to provide more clarity to its CSCs, mainly (to the extent the Cloud SP is able to do so) through transparent, contractualised statements of policy, approach and safeguards. Where cloud service provision is an element of a CSC’s contract with its own organisational or individual customers, the CSC will then be able to provide better back to back terms with its own customers.

**CSC/Cloud SP issues where the CSC is itself a regulated entity**

Although the primary focus of this paper is on investigatory powers, separate issues arise where the CSC is itself operating in a regulated environment (for example education, financial services, healthcare, professional services, transportation or utilities). Here, the CSC will be subject to its own primary duties towards its regulator, which may extend to cloud computing and fall within the elements of data sovereignty set out at paragraph A.1 above where the regulator concerned is the third party with power to access the CSC’s data. For example, regulated financial services firms in the UK are subject to a specific requirements on outsourcing which extend to the cloud, including under the SYSC 8 Senior Management Arrangements, Systems and Controls in the Handbook\(^{79}\) of the Financial Conduct Authority (FCA, the UK regulator) and when using off the shelf banking solutions\(^{80}\).

Regulated providers of legal services in the UK are also subject to specific requirements where they use the cloud, as the Solicitors Regulation Authority (SRA, the UK regulator) considers firms using Cloud services to be ‘outsourcing critical operational functions’ and so required to achieve

---


\(^{79}\) [https://www.handbook.fca.org.uk/handbook/syosc/](https://www.handbook.fca.org.uk/handbook/syosc/)

prescribed outcomes as regards contracts, clients and data. Regulators in other sectors may apply similar rules.

**CSC/Cloud SP issues where the CSC is a service provider to its regulated customer**

Whether or not they themselves are primarily regulated, CSCs may also be under secondary regulatory duties as a matter of contract where they are service providers to other primarily regulated entities. Taking the legal world again as an example, law firms are regulated entities and can be service providers to clients in other regulated sectors. For example, a bank, as a law firm’s regulated client, will be subject to its own regulatory regime, which will likely involve accountability for its data in the hands of its law firms in terms which may also require access by the bank’s regulator. Here the law firm will be accountable for data security directly to its own regulator and contractually (through its engagement terms) to its banking client, which in turn will be directly accountable to its financial services regulator.

CSCs in this position need to make sure in the relevant contracts to which they are party that these issues are satisfactorily addressed. For example, law firms should consider including in their client engagement terms an acknowledgement by their clients that the firm uses cloud services; and deal in their contracts with their Cloud SP with regulatory audit or other regulatory access to cloud data.

**Other issues: LPP etc**

CSCs like law firms, medical doctors or journalists handling through their Cloud SP LPP or otherwise privileged or confidential information should address treatment of this kind of data in the Cloud SP contract.

**Summary of CSC cloud data sovereignty contractual issues**

Discussion of data protection-related and more general cloud contract terms is outside the scope of this paper but for present purposes key CSC cloud data sovereignty contractual issues may be summarised as including:

- a contractual statement of when the CSC’s data may be subject to involuntary intrusion through the exercise of investigatory powers;
- a requirement for the Cloud SP to notify the CSC if the CSC’s data is subject to intrusion (whether through the exercise of investigatory powers, data breach or any other reason). This may of course be necessary from the CSC’s point of view if, for example, the intrusion amounts to a data breach notifiable to the CSC’s data protection or other regulator. Circumstances where notification is forbidden should also be addressed;

---

81 In the SRA Code of Conduct applicable to UK solicitors’ firms, Outcome O(7.10) equates cloud computing with critical outsourcing, setting out prescribed outcomes where the regulated firm ‘outsources legal activities or any operational functions that are critical to the delivery of any legal services’. Outcome O(7.10(b)) is that the outsourcing ‘is subject to contractual arrangements that enable the SRA or its agent to obtain information from, inspect the records (including electronic records) of, or enter the premises of, the third party, in relation to the outsourced activities or functions’ (http://www.sra.org.uk/solicitors/handbook/code/part3/content.page).
• the extent (if at all) to which the Cloud SP can, for its own or others’ purposes, use data of the CSC or its customers other than in accordance with the latters’ express instructions. Clearly, from the CSC’s point of view this possibility should be excluded so far as possible;

• whether the Cloud SP is using any subcontractors to whom CSC data is or may be disclosed, the circumstances when a subcontractor may be subject to investigatory powers and how that is notified to the CSC;

• assessing whether any Cloud SP contractual data residency, location or domiciliation commitments are subject to any exceptions (for example as to disaster recovery or business continuity purposes, use of traffic or other data, intrusion by external government agencies) and if so achieving clarity about what they are;

• if local or other data localisation laws are relevant, obtaining a statement from the Cloud SP as to how the requirements will be complied with;

• if the CSC is operating directly in a regulated sector, or for its customers in turn who are regulated, how those primary and secondary regulatory commitments (for example as to audit and access) may be complied with;

• whether and if so how LPP, privileged or otherwise confidential information will be dealt with differently from other CSC data; and

• ownership of Cloud data rights (which should reside with the CSC or its customer either as owner of the rights in relation to the data concerned or as the person giving the instructions by which the data originated).

From the above, it will be observed that the normal provider commitment about compliance with laws may be a double edged sword from the CSC’s point of view and that greater detail is needed in this area in the case of Cloud SP data sovereignty.

25. **Consumers.** Individual consumers of cloud services may be direct customers of the Cloud SPs or indirectly of CSCs. Their overriding concerns, fuelled by high profile news stories, are around data breaches generally – whether as security breaches at their provider and/or as infringement of their rights under data protection law. Data sovereignty risk is one part of this set of concerns. Individually, a consumer of cloud services will, as a practical matter, have limited scope for changing the terms of services offered by his or her provider, but when selecting service should differentiate between the different terms on offer and particularly any service providers’ policy statements in the data rights, security, protection and sovereignty areas. Collectively, consumers of course have significantly more effect with the ability to affect Cloud SPs’ market reputation and influence the terms of cloud services supply.

26. **Practical risk management: data governance and contract.** At the start of this paper (A.4) the point was made that national law based data intrusion powers exist throughout the world and are not going to go away, so there is an element of business learning to live with them. Acknowledging this from the commercial standpoint in turn grounds an approach to data sovereignty risk management that is cognitive and pragmatic. Such an approach is articulated in Gartner’s report from July 2014 quoted at paragraph A.4 about balancing the risk elements involved – legal uncertainty, fines, stakeholder dissatisfaction and innovation – and accepting a measure of residual risk. This
acceptance should not be taken as advocating a ‘do nothing’ approach to data sovereignty risk, and within limits there is much that Cloud SPs and CSCs alike can to in practically managing risk through their organisation’s approach to data governance (D.27) and contracting (D.28).

27. **Data governance.** Larger providers will view data sovereignty as part of their overall framework of data governance. Here the emphasis is on a structured approach that enables the organisation to gain maximum advantage from its data assets and operations in a secure, legally compliant way that balances rights and duties. In general terms, the structured approach will normally involve at least three elements. First, a strategy statement articulating the organisation’s rationale, goals and governance arrangements for its data; second, a policy statement that fleshes out the high level strategy statement and sets out how the data governance will be implemented; and third, more detailed day to day processes and procedures for governance operation. Data governance is developing rapidly at the moment in the area of cloud computing where, for example, the UK government has done ground breaking work for the public sector cloud around data classification,82 transposition of that classification to the Cloud83, mapping of cloud security requirements to the data classification84 and recommendation of international standards (particularly ISO 2700185 and 2701886) for assurance as to requirements compliance. This work is also likely to be of benefit to private sector organisations in their data governance.

Data governance will address data rights, data protection and data security as well as data sovereignty. From paragraph D.23 it will be observed that Cloud SPs are subject to ‘cloud as global, law as national’ - a changing, opaque, uncertain and inconsistent international legal environment based on national laws as to the scope of their duties to the ‘investigatory world’ of security and intelligence Agencies, law enforcement and other Government entities - in a commercial world where cloud business patterns are globalising. The tensions and issues arising between ‘investigatory world’ interests and the interests of customers will be best served by greater legal certainty as new laws make their way on to the statute books. Within the limits of official secrecy, data governance strategy and policy statements relating to data sovereignty, however general, as to the circumstances when customer data may be intercepted or bulk collected (and whether or not customers may be told about it) are likely to become more reassuring and conducive to building trust than silence.

---

84 https://www.gov.uk/government/publications/cloud-service-security-principles
85 The ISO 27000 series is a growing family of forty or so standards on ‘Information Technology – Security Techniques – Information Security Management Systems’ (ISMS). ISO 27001 sets out formal ISMS control objectives and controls against which an organisation can be certified, audited and benchmarked. Organisations can request third party certification assurance and this certification can then be provided to the organisation’s customers. See http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
86 ISO 27018 is a ‘Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors’ which extends the requirements of ISO 27001 in ways that are appropriate for public cloud service providers handling PII (PII is effectively the same thing as personal data in the EU). See http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
Whilst full data sovereignty governance may be some way off, Cloud SPs are increasingly using standards certification in the area of data sovereignty to build reassurance and trust. Microsoft for its Azure PaaS service for example publicises\(^87\) that it has achieved in Singapore ‘level-3 certification with the Multi-Tier Cloud Security Standard for Singapore (MTCS SS), an ISO 27001-based standard covering areas such as data retention and sovereignty’ and in New Zealand its compliance with a published ‘framework of 105 questions focused on the security and privacy aspects of cloud services that are fundamentally related to data sovereignty’. As observed above, many providers, equating data sovereignty to data location, domiciliation or residency within a particular place, publicise their services as holding data within a specified country (e.g. the UK) or area (e.g. the EEA).

From the point of view of the CSC, enterprise organisations should consider whether their operations support the development of their own cloud data location policies or jurisdiction policies. Such a policy would be the outcome of a review of the organisation’s data assets against the regulatory and business environments in the countries where it has operations, particular risks to be managed and the cost, quality and commitments offered by prospective Cloud SPs.\(^88\)

28. **Contract.** Paragraph D.24 summarised key data sovereignty issues as they arise in the Cloud SP/ CSC contractual context, and D.23 has shown why these issues may be challenging to address for the Cloud SP. Pulling back the contractual focus to more general aspects of the relationship between Cloud SP and CSC as it relates to data sovereignty, precise due diligence by the CSC as to exactly what the Cloud SPs it is inviting to tender are offering is at a premium, particularly bearing in mind the opacity and uncertainty of the legal environments providers are operating under. This means that CSC requirements should be stated as precisely as possible in pre-contractual documents and particular attention paid to tenderers’ responses. Contractual effect should then be given so far as possible to the requirements and responses. The contract should also address the particular kinds of contractual issues highlighted at D.24, focusing on any exceptions to Cloud SP obligations and remediation, remedies and redress for non-performance.

CSCs should drill down on prospective suppliers’ statements of standards compliance (for example with ISO 27001 and related standards) by making sure documents offered in evidence are up to date and cover the services the potential Cloud SP is offering and the data centres it is proposing to offer them from.

If CSCs are providing their own cloud services derived from or based on what their Cloud SP is providing to them, then relevant terms will need to be appropriately ‘back to backed’ to ensure the CSC is not bearing risk that is not offlaid.

Finally, an area of growing importance in cloud contracting is the insurance cover that the Cloud SP is required to maintain for data sovereignty and other data security risks. CSCs should consider this in the context of their own commercial general, PI (professional indemnity), data breach and business interruption policies.

---


\(^{88}\) See for example Cyberspace Law and Policy Centre, UNSW Law, Australia *Data Sovereignty and the Cloud – A Board and Executive Officer’s Guide* (July 2013).
E. CONCLUSION

29. Conclusion. The Snowden revelations, Microsoft, Schrems, Digital Rights Ireland and DRIPA litigation, and the three UK 2015 surveillance reviews have all put data interception and collection and data sovereignty laws under the spotlight as never before. This has happened just as big data and cloud computing have taken off, fuelling data globalisation and service fragmentation. The resulting 'privacy v intrusion' and 'cloud as global, law as national' debates will get fiercer in the UK as we go into 2016, with public concern increasing at each newsworthy data breach. Against this noisy background, Cloud SPs and CSCs should consider a pragmatic, cognitive approach to data sovereignty risks in their businesses. National law based data intrusion powers exist throughout the world and are not going to go away, so there is an element of business learning to live with them, balancing customer, government and other relevant interests and accepting residual risk. This is not a 'do nothing' approach however, and there is much that Cloud SPs and CSCs can do, in terms of understanding and influencing the debate and their own data governance and contracting approaches towards achieving greater transparency and certainty in the area of data sovereignty.

Richard Kemp,
Kemp IT Law, London,
October 2015
richard.kemp@kempitlaw.com
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTA</td>
<td>British Telecommunications Act 1984</td>
<td>C.13</td>
</tr>
<tr>
<td>CIA</td>
<td>US Central Intelligence Agency</td>
<td>B.7</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
<td>B.8</td>
</tr>
<tr>
<td>Cloud SP</td>
<td>cloud service provider</td>
<td>A.1</td>
</tr>
<tr>
<td>Comms SP</td>
<td>communications service provider</td>
<td>B.7</td>
</tr>
<tr>
<td>community cloud</td>
<td>cloud resources used for a community of CSCs</td>
<td>A.2</td>
</tr>
<tr>
<td>CSC</td>
<td>cloud service customer</td>
<td>A.2</td>
</tr>
<tr>
<td>DPA</td>
<td>UK Data Protection Act 1998</td>
<td>C.0</td>
</tr>
<tr>
<td>DRIPA</td>
<td>UK Data Retention and Investigatory Powers Act 2014</td>
<td>B.6, B.10, C.12</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
<td>B.8</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
<td>C.21</td>
</tr>
<tr>
<td>EU Charter</td>
<td>Charter of Fundamental Rights of the European Union</td>
<td>B.8</td>
</tr>
<tr>
<td>FBI</td>
<td>US Federal Bureau of Investigation</td>
<td>B.7</td>
</tr>
<tr>
<td>FB-I</td>
<td>Facebook’s Ireland subsidiary</td>
<td>B.8</td>
</tr>
<tr>
<td>FCA</td>
<td>UK Financial Conduct Authority</td>
<td>C.24</td>
</tr>
<tr>
<td>FISA</td>
<td>US Foreign Intelligence Surveillance Act 1978, as amended</td>
<td>B.7</td>
</tr>
<tr>
<td>GCHQ</td>
<td>UK Government Communications Headquarters</td>
<td>B.7</td>
</tr>
<tr>
<td>HRA</td>
<td>UK Human Rights Act 1998</td>
<td>C.21</td>
</tr>
<tr>
<td>hybrid cloud</td>
<td>private cloud with access to public cloud to manage peaks, etc.</td>
<td>A.2</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
<td>A.2</td>
</tr>
<tr>
<td>ICO</td>
<td>UK Information Commissioner’s Office</td>
<td>B.7</td>
</tr>
<tr>
<td>IDPC</td>
<td>Office of the Irish Data Protection Commissioner</td>
<td>B.8</td>
</tr>
<tr>
<td>IOCA</td>
<td>UK Interception of Communications Act 1985</td>
<td>C.13</td>
</tr>
<tr>
<td>IPT</td>
<td>UK Investigatory Powers Tribunal</td>
<td>C.20</td>
</tr>
<tr>
<td>IRTL</td>
<td>UK Independent Reviewer of Terrorism Legislation</td>
<td>B.7</td>
</tr>
<tr>
<td>ISA</td>
<td>UK Intelligence Services Act 1994</td>
<td>C.13</td>
</tr>
<tr>
<td>ISC</td>
<td>UK Intelligence and Security Committee of Parliament</td>
<td>B.11</td>
</tr>
<tr>
<td>ISP</td>
<td>internet service provider</td>
<td>B.7</td>
</tr>
<tr>
<td>Term</td>
<td>Meaning</td>
<td>Reference</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>LPP</td>
<td>legal professional privilege</td>
<td>C.0</td>
</tr>
<tr>
<td>MLAT</td>
<td>Mutual Legal Assistance Treaty</td>
<td>B.9, C.18</td>
</tr>
<tr>
<td>MNO</td>
<td>mobile network operator</td>
<td>B.7</td>
</tr>
<tr>
<td>MS</td>
<td>Member State of the European Union</td>
<td>B.10</td>
</tr>
<tr>
<td>NSA</td>
<td>US National Security Agency</td>
<td>B.7</td>
</tr>
<tr>
<td>OTT</td>
<td>‘Over the Top’ provider</td>
<td>B.7</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
<td>A.2</td>
</tr>
<tr>
<td>PATRIOT Act</td>
<td>US PATRIOT ACT 2001</td>
<td>B.7</td>
</tr>
<tr>
<td>PCLOB</td>
<td>US Privacy and Civil Liberties Oversight Board</td>
<td>B.7</td>
</tr>
<tr>
<td>PECR</td>
<td>Privacy &amp; Electronic Communications (EU Directive) Regulations 2003</td>
<td>C.0</td>
</tr>
<tr>
<td>private cloud</td>
<td>cloud resources used for a single CSC</td>
<td>A.2</td>
</tr>
<tr>
<td>public cloud</td>
<td>cloud resources provided on a multi-tenant basis</td>
<td>A.2</td>
</tr>
<tr>
<td>RUSA</td>
<td>UK Royal United Services Institute</td>
<td>B.11</td>
</tr>
<tr>
<td>SRA</td>
<td>UK Solicitors Regulation Authority</td>
<td>C.24</td>
</tr>
<tr>
<td>SSA</td>
<td>UK Security Services Act 1989</td>
<td>C.13</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
<td>A.2</td>
</tr>
<tr>
<td>SCA</td>
<td>US Stored Communications Act 1986</td>
<td>B.9</td>
</tr>
<tr>
<td>WTA</td>
<td>UK Wireless Telegraphy Act 2006</td>
<td>C.13</td>
</tr>
</tbody>
</table>