Cloud Computing and Data Sovereignty
Richard Kemp
March 2016
CLOUD COMPUTING AND DATA SOVEREIGNTY

TABLE OF CONTENTS

Para  Heading                  Page  Para  Heading                  Page
A. INTRODUCTION...............1  17. Extra-territorial reach: other countries’ laws 18
  1. What is data sovereignty?..........1  18. Balkenisation: a trend towards data residency,
  2. Cloud computing: the NIST definition...2  localisation and domiciliation laws? ...........19
  3. Current growth of cloud computing....3  19. Mutual Legal Assistance Treaties (MLATs), 20
  4. Data sovereignty and cloud computing: the 'privacy v intrusion' debate and managing 20. Legal Professional Privilege (LPP), etc......21
      risk................................................................4  21. No right to privacy at common law: non-
  5. Aims and scope of this white paper ...5  applicability to communications of the 1760s 21
B. DATA SOVEREIGNTY IN THE NEWS...5  warrant cases..............................................21
  6. Introduction..............................5  22. Right to privacy, etc under the ECHR, EU
  7. The Snowden allegations ...............5  Charter and data protection legislation.......22
  8. The Schrems case.......................7  D. DATA SOVEREIGNTY AND CLOUD
      etc. ...................................................7  PRACTICAL RISK MANAGEMENT........24
  10. The UK Data Retention and Investigatory  23. Data on-premise and in-cloud: isolating
      Powers Act 2014 (DRIPA) ..............11  specific cloud computing data sovereignty
      surveillance laws ..............................12  25. Relationship between Cloud SPs and
  12. The UK Investigatory Powers Bill (IPB)......13  CSCs ..................................................26
C. DATA SOVEREIGNTY: LEGAL  26. CSCs and data sovereignty issues: contracting
      BACKGROUND .....................................14  with the Cloud SP - investigatory
  13. Data sovereignty and the state’s investigatory  powers, regulatory access, etc..............27
      powers: introduction...........................14  27. Consumers......................................29
      UK law .............................................15  and contract...........................................29
  15. The framework of UK data interception and  29. Data governance .............................30
      collection ........................................16  30. Contract..........................................31
  16. The extra-territorial reach of UK data  31. Conclusion ......................................32
      interception and collection law ...........18

TABLES, ETC

Figure 1: Software as a Licence to Software as a Service: the Cloud Service Model Continuum (page 3)

Glossary (page 32)
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 legal issues principally concern the following:

- **data rights**: the intellectual property and other proprietary rights that arise in relation to data;
- **data protection**: the legal rights and duties that arise specifically in relation to personally identifiable information;
- **data security**: the mix of management, legal, technical, operational and governance controls that an organisation puts in place to ensure desired information security outcomes; and
- **data sovereignty**: a person’s right to control the disclosure of and access to his own data (whether or not the data is personally identifiable information) to a third party (typically, although not exclusively, a state agency).

For lawyers specialising in the field these issues arise most frequently in the areas of regulation, contract and governance.

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, data protection and data security are separate topics and not considered in detail here except as relevant to data sovereignty.

**Elements of data sovereignty.**

A person’s data sovereignty is violated when a third party is using data in breach of another person’s contractual, intellectual property or other rights or in a way that causes that other person to be in breach of their own legal or regulatory duties. More specifically a breach of data sovereignty is likely to happen in a situation where:

- a third party (typically but not always a government agency)
- has the power to access the data of another person (for example, a corporate or individual cloud 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.

A breach of data sovereignty can happen:

- **on-premise**, for example on a server or a personal device owned or used by the cloud customer;
- or
- **in-cloud**, on a server owned by the cloud service provider or during transmission between servers or between a cloud server and a customer device.

This paper focuses on issues raised by in-cloud breaches of data sovereignty – whether in transit to or from the cloud or stored or processed in the cloud.

Stakeholders in the data sovereignty discussion

Data sovereignty affects four main types of actor:

- **government agencies** are concerned principally with the scope of their powers to access data, the authorisations required to exercise those powers, and the agency's accountability for their use;
- **cloud service providers (Cloud SPs)** have concerns about:
  - retaining customer trust and their own reputation in the market (reputational concerns); and
  - contract terms, policies, governance and compliance with legal requirements (operational concerns);
- **corporate cloud service customers (CSCs)** share Cloud SPs’ reputational concerns but are generally obverse to them in contractual and policy terms; and
- individual cloud customers are mainly concerned about data security and unauthorised access to their data.

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 definition\(^1\) of cloud computing by the US National Institute of Standards and Technology (NIST) specifies a type of computing with five key characteristics, three service models and four deployment models. The key characteristics are:

- **on-demand self-service**: the customer can obtain computing capabilities automatically as needed without intervention by the Cloud SP;
- **broad network access**: computing capabilities are available over the network and accessed through standard mechanisms anytime, anywhere;
- **resource pooling**: the Cloud SP’s computing resources are pooled to serve multiple customers using a multi-tenant model which results in cost reduction through leveraging economies of scale.

\(^1\) available at [http://www.nist.gov/itl/cloud/](http://www.nist.gov/itl/cloud/)
• **rapid elasticity**: computing capabilities can be quickly scaled out or scaled in depending on the CSC's needs. This allows the CSC to respond to business demand without taking the risk that they will be over or under sourced; and

• **measured service**: The CSC's resource usage can be monitored and controlled and it pays for what it uses.

The elements of the **Software as a Service** (SaaS), **Platform as a Service** (PaaS) and **Infrastructure as a Service** (IaaS) service models are shown at 1, 2 and 3 in Figure 1 below.

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

The four deployment models are:

• **private cloud**: where infrastructure, platform and/or software are used solely for a single CSC;

• **community cloud**: used solely 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**: as private cloud with access to public cloud to manage peaks.

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”.2

---

Driven by these factors, cloud computing is currently at an inflexion point and by the start of 2016 has become the ‘new normal’. Recent results 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 around 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.³


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’. Concerns have been further heightened by regular news stories about hacking⁴ (whether of on-premise or in-cloud systems).

To put the “privacy v intrusion” debate into context from a practical point of view and to refine the steps that businesses may take to mitigate the data sovereignty risks highlighted in this paper, affected stakeholders should bear in mind the following. First, although the Snowden revelations centred on the USA, the alleged state surveillance and data intrusion powers are likely to exist across the world. Second, at root, government sees those surveillance powers as the contemporary expression of powers to keep the country safe that have always existed in the offline realm to ensure public and national security. Businesses may therefore need to follow a pragmatic approach to data sovereignty risk management. In the words of research firm Gartner from July 2014:⁵

“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.”

⁴ A 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.
Aims and scope of this white paper. This paper is designed to overview the issues that are relevant and to set out the practical steps that businesses should take in order to mitigate the risks of adverse action that they and their customers may face. 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. This paper is written as at 1st March 2016 (replacing the first September 2015 and January 2016 versions) and from the perspective of English law, making reference where relevant to the laws of other countries. It will be updated again when the new UK Investigatory Powers Bill published on 1st March 2016 has received the Royal Assent.

B. DATA SOVEREIGNTY IN THE NEWS

6. Introduction. Issues touching on data sovereignty have made headlines since mid-2013 when Edward Snowden published his allegations about the bulk information collection programmes of US and UK security services (paragraph B.7 below). In the years that followed there have been several developments at both legislative and judicial level that have brought the issue of data sovereignty into sharp focus. They include the following:

- the action brought by Austrian student Max Schrems before the Irish High Court in which he challenged the Irish Data Protection Commissioner’s decision that it was not required to investigate complaints that the transfer of personal data by Facebook Ireland to its US parent company Facebook Inc. violated EU data protection law (B.8 below);
- Microsoft’s ongoing litigation over the warrant to obtain information for US proceedings from its Dublin data centre, In Re Warrant (B.9);
- the UK High Court’s decision 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) and the publication of the UK Investigatory Powers Bill in November 2015 (B.12).

All these 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 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). Except for the PRISM programme, the UK Government has assumed a strict policy of ‘neither confirm nor deny’.

The US programmes were said to be authorised in the USA under s215 Patriot Act 2001 and s702 Foreign Intelligence Surveillance Act 1978, as amended (FISA). At the time, the Patriot Act programme authorised 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. The USA Freedom Act of June 2015 has since made a number of modifications to the provisions of section 215, albeit that they concerned limitations on bulk collection by US intelligence agencies of communications data relating to US citizens only.

**PRISM.** Media attention has largely focused on data collection under the ‘PRISM’ programme, a s702 FISA programme operated by the NSA under the authority of the US Attorney General and Director of National Intelligence. Under the programme it is said that nine US internet companies are compelled to provide data extending beyond metadata (including email, chat, videos and video conferencing, photos, stored data, VOIP (but not other telephone) calls and social networking details) to the NSA directly from their servers. 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.

**UPSTREAM.** A second s702 FISA collection programme, ‘UPSTREAM’, is said to involve compelled assistance from communication service providers (Comms SPs) as the operators of the

---


7 Mr Snowden was the subject of a BBC Panorama television programme, ‘Edward Snowden: Spies and the law’ transmitted on 5 October 2015.


9 Said to be AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo and YouTube.

10 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 development 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
telecommunications backbone over which messages are communicated, upstream of the PRISM internet companies.

**TEMPORA.** ‘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. Between 10% and 25% of global telecoms and internet traffic is estimated to transit the country via these cables. The data collected is similar to that provided under PRISM and there were alleged to be 46 cables (out of an estimated global total of 100,000 bearers) tapped in this way in 2012.11 Disclosure of the PRISM programme has caused international consternation with attention centring on the following:

- The programme’s legal basis and 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 EU, this has centred on EU data protection rules and the extent to which US law enforcement agencies can access personal data of UK and other European citizens. 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) said12:

“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. **The Schrems case.** The case of *Maximilian Schrems v Data Protection Commissioner* 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.13 The IDPC carried out an audit of FB-I, publishing its report in December

services described in this footnote. With these reservations, the terms are used in this sense in this white paper.

13 See [http://europe-v-facebook.org/EN/Complaints/complaints.html](http://europe-v-facebook.org/EN/Complaints/complaints.html) for the complaints.
2011. The report contained 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. In particular, the IDPC argued that it was bound by the European Commission’s findings in Decision 2000/520 that Safe Harbor ensured adequate protection. 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, the judgement also found that although the electronic surveillance and interception of personal data...
transferred from the EU to the US served necessary and indispensable objectives in the public interest, the revelations made by Edward Snowden had demonstrated a "significant over-reach" on the part of the NSA and other federal agencies. In addition, the court found that EU citizens had no effective right to be heard as part of US oversight proceedings. As a result, the court considered that Decision 2000/520 did not satisfy the requirements flowing both from Articles 7 and 8 of the Charter. The judge, therefore referred the case to the Court of Justice of the European Union (CJEU) because of the critical issue that arose:

"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."22

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, delivered his opinion 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 201523. The CJEU ruled that a Commission decision adopted pursuant to Article 25(6) of the Data Protection Directive, like Commission Decision 2000/520/EC, does not prevent a supervisory authority of a member state from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, which has been transferred from a member state to that third country, when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection. In the process it also held that Decision 2000/520 was invalid. Following the ECJ judgment, the DPC has now agreed to investigate the complaint.

The ECJ’s judgment resulted in immediate responses, most notably from the European Commission and the Article 29 Working Party on 16 October 201524. The Working Party issued a statement calling for or intergovernmental talks between member states, EU institutions and US authorities to find solutions enabling EU-US data transfers that respect fundamental rights. It confirmed that that while it analysed the impact of the judgment on alternative data transfer mechanisms, the Standard Contractual Clauses and Binding Corporate Rules can still be used. However, it further stated that unless a resolution with the US authorities was reached by the end of January 2016 and depending on its assessment of alternative data transfer mechanisms, EU data protection authorities could take enforcement action where necessary or appropriate. The European Commission on 6 November 2015 published an explanatory Communication on the impact of the Schrems case25.

---

22 Paragraph 84
9. **Microsoft v United States: In re Warrant etc.** In December 2013, US federal prosecutors during the course of a narcotics criminal investigation obtained an authorisation under the US Stored Communications Act 1986 (SCA) from a federal Magistrate in New York 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.26 On 5 September 2014, Microsoft 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 international 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, 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 Government27. Judgment is expected within the next few months.

---

26 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/

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\(^28\) that s1 DRIPA was incompatible with the judgment of the CJEU in case C-293/12 (\textit{Digital Rights Ireland Ltd}).\(^29\)

In \textit{Digital Rights Ireland} the CJEU had to consider whether the EU Data Retention Directive 2006/24\(^30\) 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 held that the retention requirements in the Directive constituted an interference with both the right to a private life and the right to data protection and that although this interference satisfied an objective of general interest, it did not comply with the principle of proportionality set out in Article 52 (1) of the Charter. The court 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\(^31\) (broadly, Comms SPs) and the other for internet access, telephony and email (broadly, ISPs and certain OTTs).\(^32\) 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\(^33\) received the Royal Assent and came into force on 17 July 2014. S1 DRIPA was the replacement provision for the regulations struck down in \textit{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


\(^33\) http://www.legislation.gov.uk/ukpga/2014/27/contents
June and 9 July 2015. Judgment was given on 17 July, when the High Court allowed the application, holding that s1 DRIPA 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.

The Government appealed to the Court of Appeal and on 20 November 2015 the Court of Appeal referred to the ECJ the questions whether the ECJ in *Digital Rights Ireland* intended first to set out mandatory requirements that MS had to comply with in their national legislation and secondly to extend Articles 7 or 8 of the EU Charter further than the interpretation of Article 8 of the ECHR as established by the case law of the European Court of Human Rights (ECTHR).

11. **Review of UK telecoms and internet surveillance laws.** As if to pave the way for this debate, three reports were 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 reviewed 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 articulated 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 recommended an overhaul of the UK’s legislation.

---

35 http://isc.independent.gov.uk/committee-reports/special-reports
12. **The UK Investigatory Powers Bill (‘IPB’).** In May 2015, the UK government announced plans in the Queen's Speech to publish a new IPB. The Bill is designed to close "capability gaps" in the area of interception and communications data retention, and to maintain the ability of the intelligence agencies and law enforcement to target the online communications of terrorists and other serious criminals. Following previous announcements and the government's defeat in the case of *Davis and others* (paragraph B.10 above) the IPB includes a replacement regime for section 1 DRIPA as well as an extension of the data retention requirement to other types of data like data generated in the context of social media use. In addition, the IPB will form part of a review of investigatory powers and their regulation that is required under section 7 of DRIPA.

A new draft bill was originally presented to Parliament by the Secretary of State on 4 November 2015. The bill attracted widespread comment and was the subject of recommendations made by parliamentary committees including the ISC and the Joint Select Committee on the Draft Investigatory Powers Bill. 38 Responding to Committees’ call for greater legislative clarity, stronger privacy safeguards and more developed internet record retention plans, the Secretary of State published on 1 March 2016 a revised bill, along with a number of overarching documents and codes of practice 39.

The passage of the bill through Parliament is unlikely to be particularly smooth. This White Paper will be updated when the new law has received the Royal Assent. The main points of the draft legislation are as follows:

- it aims to consolidate the previous patchwork of laws under one new statute;
- it will enshrine in primary legislation for the first time protection for communications involving ‘sensitive professions’ including lawyers, medical doctors, journalists and MPs;
- it will require communications service providers to retain communications data for up to 12 months;
- it will for the first time expressly authorise equipment interference (hacking) and bulk data collection by the security services;
- oversight will be improved:

38 The Committee has published on its website more than one hundred responses and submissions on the IPB received from interested parties. Available at [http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/publications/?type=Written#pnlPublicationFilter](http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/publications/?type=Written#pnlPublicationFilter)


The government has also published a number of draft codes of practice, available at [https://www.gov.uk/government/publications/investigatory-powers-bill-codes-of-practice](https://www.gov.uk/government/publications/investigatory-powers-bill-codes-of-practice). They are (i) National security notices: draft code of practice; (ii) Interception of communications: draft code of practice; (iii) Security and intelligence agencies retention and use of bulk personal datasets: draft code of practice; (iv) Equipment interference: draft code of practice; (v) Communications data: draft code of practice; and (vi) Bulk acquisition: draft code of practice.
the current unwieldy structure of separate oversight commissioners will be replaced by a new Investigator Powers Commissioner, who will be supported by senior judges as Judicial Commissioners and a staff of experts;

- the Judicial Commissioners panel will have a power of veto over the authorisation of interception, equipment interference and bulk data collection warrants, with an exception for urgent cases of up to five days where the Home Secretary alone may grant authorisation. The scope of this exception is likely to be a focus of debate; and

- the Judicial Commissioners will required to publish an annual report.

A new domestic right of appeal to the Investigatory Powers Tribunal will be introduced.

C. DATA SOVEREIGNTY: LEGAL BACKGROUND

13. 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 outsides 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.14 - C.20 below) and then citizens’ rights (C.21 and C.22). Paragraph C.14 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.16) and other countries (C.17) is then briefly considered, followed by a quick look at the trend towards national data residency, localisation or domiciliation laws (C.18), mutual legal assistance treaties (MLATs) (C.19) and treatment of legal professional privilege (LPP) and related issues (C.20). As to citizens’ rights, in the absence of protection at common law for the privacy of communications (C.21), 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.22.40

40 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.
The State’s Powers

14. **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 action\textsuperscript{41}, 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 (and for the previous seventy years had been) the monopoly of the state-owned General Post Office. Since then, telecommunications has been progressively and extensively liberalised and deregulated\textsuperscript{42}, the UK intelligence Agencies have been formally avowed and put on a statutory footing\textsuperscript{43} and communications interception has been made subject to legislation.\textsuperscript{44}

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\textsuperscript{45}, it is in exercise of a warrant or statutory power properly conferred or it is otherwise authorised.\textsuperscript{46} 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 (**RIPA**),\textsuperscript{47}
- powers to intercept wireless communications are also conferred under ss48 and 49 WTA\textsuperscript{48} with

\textsuperscript{41} 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.

\textsuperscript{42} 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**).


\textsuperscript{45} S1(1) and (3) RIPA, ss48(1) and (3) WTA.


further broad powers provided for by s94 BTA\(^{49}\); 

- specific public authorities have numerous other powers to gather data\(^{50}\); 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 to B.12, 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 them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and - in the long run - intolerable.”

15. **The framework of UK data interception and collection law**. The core concepts in the UK legislation 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**

Interception is the monitoring or collecting of the ‘content’ of a communication ‘in the course of transmission’\(^{51}\). ‘Content’ is not defined (as distinct from communications data, which is) but includes everything to do with the communication and its related communications data\(^{52}\); broadly, content is the message along with its associated metadata as the envelope. Importantly ‘in course of transmission’ includes any time when the communication is stored so that the intended recipient can access it.\(^{53}\) 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 cover\(^{54}\) 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.

\(^{50}\) See IRTL Report, Annex 6, List of Bodies with non-RIPA powers, pages 323 to 330.  
\(^{51}\) s2 RIPA  
\(^{52}\) s20 RIPA  
\(^{53}\) s2(7) RIPA  
\(^{54}\) s20(4) RIPA
**Interception powers**

RIPA interception powers can only be applied for by a limited number of specified services\(^\text{55}\), 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\(^\text{56}\). 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\(^\text{57}\).

**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 disapplied by the High Court on 17 July 2015 on a delayed basis until 31 March 2016 for the same reasons as the previous rules and will be replaced when the IPB becomes law.

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 State\(^\text{58}\).

**‘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

---

\(^{55}\) 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.

\(^{56}\) s5(3) RIPA

\(^{57}\) IRTL Report, paragraph 6.43 page 106. See also paragraph B.7 above in relation to TEMPORA.

\(^{58}\) See [https://www.gov.uk/government/collections/ripa-codes](https://www.gov.uk/government/collections/ripa-codes)
internal and external communications is less clear, giving rise to increasing interpretation difficulties in a world where global services are growing fast.

16. **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)\(^{59}\) 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 OTT\(^{60}\) 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.

**Interception**

As regards interception, a person (the service provider concerned) is required\(^{61}\) 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. 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.\(^{62}\)

**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.”

17. **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.14 to C.16 above

---

\(^{59}\) 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.  

\(^{60}\) See footnote 14 for an explanation of these terms and how they are used in this white paper.  

\(^{61}\) Under s11 RIPA as amended by s4 DRIPA  

\(^{62}\) s12 RIPA as amended
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.63

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 the Digital Rights Ireland case (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 Bill64 which was approved by the French Conseil Constitutionnel on 23 July 201565. 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.

18. **Balkanisation: 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 balkanisation or national residency, localisation or domiciliation laws to enforce the retention of data in the country of

---

63 See also footnote 11 above on the impact of the USA Freedom Act on s215.

64 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)

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.66 **China**67 and **Vietnam**68 have also passed data localisation laws.

19. **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. The US December 2013 report *Liberty and Security in a Changing World*69 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:

67 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)
69 See footnote 10
“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.”

20. **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’.

The Acquisitions and Disclosure of Communications Data Code of Practice states that while data is not subject to any form of professional privilege the degree of interference with an individual’s rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information. It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist. Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. This question is also dealt with further in the IPB.

**Citizens’ Rights**

21. **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 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*70 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

___________________________

70 98 ER 489, [http://www.bailii.org/ew/cases/EWHC/CP/1763/J95.html](http://www.bailii.org/ew/cases/EWHC/CP/1763/J95.html), judgment of 6 December 1763

Cloud Computing and Data Sovereignty (Kemp IT Law, v.2.1, Mar 2016)
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*.71 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 UK72 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 courts73 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.

22. **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 199874 (**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 in the UK courts as ‘Convention rights’ under the HRA. In this context, the courts must ‘take into account’ case law of the ECtHR (s2(1)) and interpret UK legislation compatibly with the ECHR (s3(1)). Where they find that UK law does violate Convention rights they can make a ‘declaration of incompatibility’ (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.

---

71 95 E.R. 807, [http://www.bailii.org/ew/cases/EWHC/KB/1765/J98.html](http://www.bailii.org/ew/cases/EWHC/KB/1765/J98.html), judgment of November 1765

72 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.


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. This means that the CJEU may declare EU legislative acts (decisions, regulations and directives) invalid 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:

> “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.”

Examples for the impact of the Charter on member states’ surveillance activities include:

- the CJEU’s decision in *Digital Rights Ireland*, where it declared the Data Retention Directive invalid (B.10 above);
- the CJEU’s decision in *Schrems*, where it held that the Safe Harbor Decision 2000/520 on the Safe harbor was invalid (B.8); and
- the UK High Court’s decision in *Davis and others*, where the court found DRIPA to be incompatible with the CJEU’s decision to declare the Data Retention Directive invalid (B.10).

**Data protection legislation**

The Data Protection Act 199875 (DPA, calling down into UK law the Data Protection Directive) and the Privacy and Electronic Communications (EU Directive) Regulations 200376 (the PECR, calling down the related EU directive77) 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’.78 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 by the new General Data Protection Regulation (“GDPR”). On 15 December 2015, the EU Commission, Parliament and Council of Ministers reached agreement on the text of the GDPR after four months of negotiations in trilogue. It will be published in the EU Official Journal in early 2016 and enter into effect two years later.

Other rights

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.

D. DATA SOVEREIGNTY AND CLOUD COMPUTING: SPECIFIC ISSUES AND PRACTICAL RISK MANAGEMENT

23. 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 for storing or processing personal data, data in its own server room or data centre may potentially be subject to interception by third parties. The organisation’s communications (in common with organisations across the UK) may be subject to bulk collection through the TEMPORA fibre optic cable interception programme (if the Snowden allegations are accurate in this respect); communications data of the

---

78 https://ico.org.uk/about-the-ico/
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 as the same rules will apply wherever the location of processing and storage. Other potentially tortious or criminal activity like hacking, denial of service, malware or screen-scraping may constitute a risk to 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 storage and processing of data.

However, 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.24 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 obverse to that of the Cloud SP and is largely concerned with the protection of its own right to privacy and data protection (in the case of individuals) and its compliance with applicable data protection laws (in the case of businesses) (D.26). For each, practical risk management steps are considered at D.28 to D.30.

24. 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. A preliminary issue, particularly as regards the developing area of OTTs, is therefore to determine which types of Cloud SPs are caught by the various investigatory powers nets at all. The next step is that the current framework of investigatory powers law is based on national laws so that a Cloud SP within the net operating internationally is subject to a wide and potentially inconsistent array of legal requirements. There is therefore a tension for a Cloud SP with international operations between ‘cloud as global, law as national’ which may be summarised in the following layered way:

- **Layer 1: access to domestic data centres by domestic agencies.** Data stored or processed in data centres situated in a Cloud SP’s country of establishment is likely to be subject to intrusion by that country’s public authorities under that country’s laws (including the interception of communications by government agency, communications data collection and other exercise of investigatory powers). [Example: in the UK, access to data held in UK data centres may be permitted under RIPA.]

- **Layer 2: access to foreign data centres by domestic agencies.** Domestic law may grant the public authorities of a Cloud SP’s home country the right to access data stored in any data centre under its control in another country. [Example: in the Microsoft *In re Warrant* case (B.9) US law...
enforcement agencies are seeking to obtain access to data held on Microsoft’s Irish data centre under the SCA.]

- **Layer 3: access to foreign data centres by foreign agencies.** Access to data held in data centres located in a third country or where a subsidiary operating that data centre is registered or otherwise located may also be granted to public authorities of that country under that country’s laws. **[Example: RIPA may authorise under warrant law enforcement agencies in the UK to intercept or collect data stored at a UK data centre operated by a US company.]**

- **Layer 4: extraterritorial access.** Data stored or processed in the cloud may also be subject to access by a government agency from any country under that country’s laws while in transit through that country. **[Example: bulk (or external) warrants issued under s8(4) of RIPA authorise interceptions where the communication sender(s) or recipient(s) are outside the British Islands.]**

- **Layer 5: compliance with layers 2 to 4 risk breaching another country’s law.** In granting one agency access to data the Cloud SP risks breaching laws of another country to which it is subject. **[Examples: the positions of FB-I at B.8 and Microsoft at B.9.]**

- **Layer 6: impact of data domiciliation requirements.** A Cloud SP may also be subject in one or more of countries to any specific residency, localisation or domiciliation requirements for data originating in that country’s territory **[Example: Russian law requires operators using servers to collect, aggregate, store, update and extract personal data of Russian citizens to locate those servers in Russia].**

25. **Relationship between Cloud SPs and CSCs.** 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 will 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, LinkedIn and Twitter) advocate the adoption of five principles79 which address:

- limiting government authority to collect users’ information;
- oversight and accountability;
- transparency about government demands;
- respecting the free flow of information; and

---

79 [https://www.reformgovernmentsurveillance.com/](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\(^{80}\) or restricting data storage to a particular country, region or geography\(^{81}\).

26. **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, with regard to its agreements with those customers.

**Investigatory powers and Cloud SP contracts**

How Cloud SPs should deal with CSC data in relation to the exercise by government agencies of investigatory powers is as yet relatively undeveloped in contracts between Cloud SPs and CSCs. This is an area where increased underlying legal certainty regarding the relationship between the primary government agency and the Cloud SP 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 agree back to back terms with its own customers.

**Contractual issues where the CSC is itself a regulated entity**

Separate issues may arise where the CSC is itself operating in a regulated environment (for example education, financial services, healthcare, professional services, transportation or utilities). In this case, the CSC will be subject to its own primary duties towards its regulator, which may extend to the treatment of data stored or processed in the cloud. For example, regulated financial services firms in the UK are subject to a specific requirements on outsourcing which extend to the cloud, including provisions regarding oversight under the SYSC 8 Senior Management Arrangements, Systems and Controls in the Handbook\(^{82}\) of the Financial Conduct Authority (**FCA**, the UK regulator) and when using off the shelf banking solutions\(^{83}\). More specifically, in November 2015, the FCA issued Guidance Consultation 15/6 on proposed guidance for firms outsourcing to the cloud and other third-party IT services.\(^{84}\)

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

---


\(^{82}\) [https://www.handbook.fca.org.uk/handbook/sysc/](https://www.handbook.fca.org.uk/handbook/sysc/)


\(^{84}\) [https://www.fca.org.uk/static/documents/guidance-consultations(gc15-06.pdf](https://www.fca.org.uk/static/documents/guidance-consultations(gc15-06.pdf)
using Cloud services to be ‘outsourcing critical operational functions’. Legal services providers are therefore required to achieve prescribed outcomes as regards contracts, clients and data. Regulators in other sectors may apply similar rules.

**Contractual issues where the CSC’s customer is a regulated entity**

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. For example, law firms are regulated entities and can be service providers to clients in other regulated sectors like banking, accountancy or healthcare. The 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. That regulator may also require access to that data. In this case 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 regulator.

CSCs in this position must make sure that these issues are adequately addressed in the relevant contracts with its own customers. 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 data security requirements, regulatory audit and other regulatory access to cloud data.

**Other contractual issues: LPP etc**

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

**Summary of contractual issues**

Discussion of data protection-related and more general cloud contract terms is outside the scope of this paper but for the purpose of protecting their data sovereignty in the cloud, CSCs should consider including the following provisions into their contract with Cloud SPs:

- 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 that the CSC must notify to its national data protection or other regulator. Circumstances where notification is forbidden should also be addressed;

---

85 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).
• a provision clarifying whether and the extent to which the Cloud SP can use data of the CSC or its customers for its own or others’ purposes otherwise than in accordance with the CSC’s express instructions. Clearly, from the CSC’s point of view this possibility should be excluded so far as possible;

• a provision clarifying 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 (if at all) access to the CSC’s data on the basis of those powers is notified to the CSC;

• a provision confirming whether any contractual commitments by the Cloud SP with regard to data residency, location or domiciliation 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 a clarification of those exceptions;

• a provision clarifying if local or other data localisation laws are relevant, in particular a statement from the Cloud SP as to how it will comply with any such requirements;

• a provision clarifying if the CSC is operating directly in a regulated sector, stores or processes data on behalf of customers that are themselves regulated entities or members of regulated professions. The provision should set out how those primary and secondary regulatory commitments (for example as to audit and access) will be complied with;

• a provision detailing what safeguards the Cloud SP will provide with regard to LPP, privileged or otherwise confidential information; and

• a provision detailing who owns what rights in the cloud data (which should ideally 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.

27. **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 likely to be 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 a service consumers should ideally differentiate between the providers’ terms of business and any other policy statements regarding data rights, data security, data protection and data sovereignty. Collectively, consumers do of course have significantly more influence with the ability to affect Cloud SPs’ and corporate CSCs’ market reputation and may thereby influence the terms of cloud services supply.

28. **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 should result in 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 do in practically managing risk through their organisation’s approach to data governance (D.29) and contracting (D.30).

29. **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 in the area of cloud computing is developing rapidly. For example, the UK government has done ground breaking work for the public sector cloud around data classification, transposition of that classification to the Cloud, mapping of cloud security requirements to the data classification and recommendation of international standards (particularly ISO 27001 and ISO 27018) 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. 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 collected in bulk (and whether or not customers may be notified of this) are likely to become more reassuring and conducive to building trust than silence.

Whilst full data sovereignty governance may be some way away, Cloud SPs are increasingly using standards certification in the area of data sovereignty to build reassurance and trust. Microsoft for

---

89 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](http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)
90 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](http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498)
its Azure PaaS service for example publicises\(^91\) 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.\(^92\)

30. **Contract.** Paragraph D.26 summarised key data sovereignty issues as they arise in the Cloud SP/CSC contractual context, and D.24 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.26, 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) in sufficient detail and make sure that 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.


\(^92\) 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

31. Conclusion. The Snowden revelations, Microsoft, Schrems, Digital Rights Ireland and DRIPA litigation, and the three UK 2015 surveillance reviews and UK IPB 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 in 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,
March 2016
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.14</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>B.7</td>
</tr>
<tr>
<td>DRIPA</td>
<td>UK Data Retention and Investigatory Powers Act 2014</td>
<td>B.6, B.10</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>B.10</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>B.7</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>GDPR</td>
<td>General Data Protection Directive</td>
<td>C.22</td>
</tr>
<tr>
<td>HRA</td>
<td>UK Human Rights Act 1998</td>
<td>C.22</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.14</td>
</tr>
<tr>
<td>IPB</td>
<td>UK Investigatory Powers Bill</td>
<td>B.12</td>
</tr>
<tr>
<td>IPT</td>
<td>UK Investigatory Powers Tribunal</td>
<td>C.21</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.14</td>
</tr>
<tr>
<td>ISC</td>
<td>UK Intelligence and Security Committee of Parliament</td>
<td>B.11</td>
</tr>
<tr>
<td>Term</td>
<td>Meaning</td>
<td>Reference</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>ISP</td>
<td>internet service provider</td>
<td>B.7</td>
</tr>
<tr>
<td>LPP</td>
<td>legal professional privilege</td>
<td>C.20</td>
</tr>
<tr>
<td>MLAT</td>
<td>Mutual Legal Assistance Treaty</td>
<td>B.9, C.19</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.22</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>RUSI</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.25</td>
</tr>
<tr>
<td>SSA</td>
<td>UK Security Services Act 1989</td>
<td>C.14</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.14</td>
</tr>
</tbody>
</table>