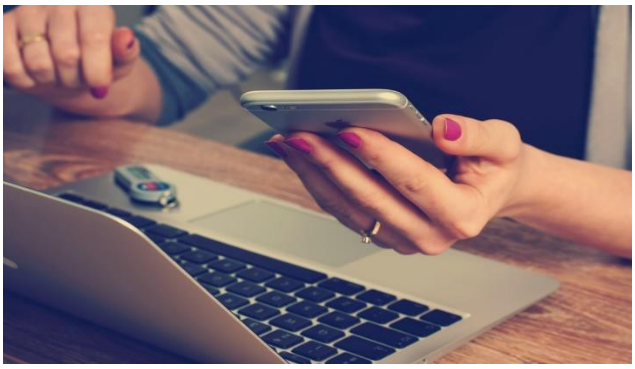
UK Parliament
POST

POSTNOTE
Number 629 June 2020

Cloud Computing



Cloud computing refers to the delivery of computing services (such as data storage and processing) on-demand over the internet. This POSTnote describes the different types of cloud computing before outlining issues relating to security, regulation, energy use and barriers to the adoption of this technology.

Overview

- Cloud computing describes the provision of computational resources as a service over the internet. Most UK organisations now use cloud computing in some capacity.
- Cloud computing offers security benefits, but improper use of cloud services can lead to data leaks.
- Organisations may face resiliency and lock-in risks by being over-dependent on a single cloud service provider.
- Cloud computing can offer energy savings, enabling organisations to reduce their carbon footprint.
- Barriers to the adoption of cloud computing include a lack of skills to buy and manage cloud services.

Background

Cloud computing is the use of pooled, centralised computing resources (including data storage and processing) that are provided to customers on-demand, often over the internet. This allows consumers and organisations to access a range of computing services without needing to own and maintain specialised hardware and software. Cloud computing, also referred to as 'the cloud' or simply 'cloud', first became commercially available in 2006.[1] Mainstream consumer services, such as those used for media streaming (e.g. Netflix, Spotify and YouTube), online document editing (such as Google Docs), file storage (including Dropbox and Google Drive), social networks (such as Facebook and Skype) and email (such as Gmail) are all enabled by cloud computing. For organisations, cloud services are available for managing databases, logistics, customer information and relations, as well as office applications (e.g. Microsoft Office 365) and video conferencing tools (e.g. Zoom), which can help facilitate remote and collaborative working.[2] Cloud computing offers organisations an alternative to buying and managing their own hardware, which can lead to reduced IT costs and the ability to access as many computing resources as they need. Many stakeholders have cited cloud computing as a key enabler of next generation technologies like big data analytics (POSTnote 468), artificial intelligence and the Internet of Things (POSTnote 593).[3]

The UK cloud market is forecast to be worth over £35 billion by 2023 (a 73% rise from 2019).[4] A 2018 survey from the Cloud Industry Forum found that 89% of larger UK organisations use at least one cloud-based service.[3] The same survey found that, in 2018, UK businesses' spending on cloud services had surpassed their spending on on-premise computing facilities for the first time. However, a Eurostat survey of small private enterprises, also carried out in 2018, found that only 39% used cloud computing, indicating that smaller organisations may not be adopting the cloud as quickly as larger ones. In 2013, the UK Government introduced the Cloud First policy to encourage the use of cloud computing in the public sector.[5] This policy mandates that central government departments must consider cloud before any other IT implementation option, and it is recommended for all UK public sector organisations.[5–7]

This POSTnote reviews commonly used types of cloud services before discussing issues surrounding security and resilience, regulation, energy use and barriers to adoption, focusing on how these issues affect public and private sector organisations.

Cloud services

Cloud computing can be implemented in different ways to suit the needs of different users. Implementations include:

- **Private clouds:** Built for the exclusive use of a single organisation and tailored to the organisation's needs. These clouds may be built, owned or operated by the organisation itself or by a cloud service provider (CSP).[8] Private clouds are often used by larger organisations handling large or sensitive datasets. Private clouds make up 22% of the UK cloud market.[4]

- **Public clouds:** Built, owned and operated by a CSP and provided to any individual or organisation on a pay-as-you-go basis over the internet.[8] Organisations that wish to scale their business on demand and in a cost-effective manner may use public cloud. Some of the most prominent public CSPs are large-scale US companies with a multinational presence such as Amazon, Microsoft and Google (Box 1).[9] It has been predicted that, by 2025, 49% of the world's data will be stored in public clouds.[10] Public clouds account for 48% of the UK market.[4]
- **Hybrid clouds:** The use of a combination of public and private clouds and on-premise computing that work together to perform the same tasks.[8] Hybrid clouds allow organisations to move applications and data around depending on their requirements. Hybrid clouds make up 30% of the UK market.[4]
- **Multi clouds:** The use of a combination of multiple public or multiple private clouds, sourced from different CSPs, where each cloud is used for an independent task.[11] Multi clouds can allow an organisation to optimise each cloud service for its specific task and prevent them from becoming over-reliant on a single provider.

75% of large UK organisations that use cloud computing use more than one cloud service, indicating a trend towards hybrid and multi cloud implementations.[3,12] In addition to the different implementations, cloud services are typically offered as one of three service models.[8,13] These are:

- **Infrastructure as a Service (IaaS):** The CSP maintains the computational hardware and offers this to users as remote computing infrastructure. The user can choose and control the operating system and applications as they would with a physical computer. IaaS is useful for organisations with strong in-house IT skills who want ready access to powerful computing. For example, the accommodation service Airbnb is built on IaaS from Amazon.[14] IaaS accounts for 28% of the UK market.[4]
- **Platform as a Service (PaaS):** The CSP provides the user with a platform where they can develop, test and deploy their own applications. Applications can be rapidly scaled up in a cost-effective manner as demand grows, making PaaS popular with application developers. PaaS makes up 9% of the UK market.[4]
- **Software as a Service (SaaS):** The CSP also manages the data and applications, offering ready-to-use software that performs specific tasks, such as Dropbox for file sharing and storage, Microsoft Office 365 and Gmail. Typically, users only have limited controls over the software. Consumers predominantly interact with the cloud through public SaaS. SaaS accounts for 63% of the UK cloud market.[4]

Infrastructure

Cloud computing is provided by dedicated data centres run by national or international CSPs. Access to these data centres is directly dependent on the national and cross-border telecommunications infrastructure.

Box 1: The cloud industry in the UK and abroad

The global public infrastructure as a service and platform as a service markets are currently led by Amazon Web Services and Microsoft Azure.[15–17] In the software as a service market the biggest shares are held by Microsoft and Salesforce.[18] There are many national cloud service providers within the UK, however none have a significant global market share.[19]

Concerns over the dominance of large US cloud service providers in providing cloud services to the UK public sector have been reported.[20–22] Some stakeholders, including a former Minister for Digital and the Creative Industries and the CEO of UKCloud (a prominent provider of cloud services to the public sector), have called for the UK to establish a sovereign cloud capacity.[23,24] The European Commission has proposed funding for a pan-European, sovereign cloud initiative.[19] In October 2019, GAIA-X, an initiative to establish a sovereign European cloud was announced.[18] Some stakeholders advocate for global clouds as they have benefits such as the flexibility to scale globally.[27,28]

Data centres

Data centres are buildings designed to house large numbers of computer systems and to guarantee certain levels of power supply, network access, security and backup equipment. CSPs may rent space within a shared facility or build their own data centres. Some CSPs rent out their data centre space for organisations to run private clouds. Data centre locations are intended to be highly secure; users may be bound by non-disclosure agreements to protect their location.[29]

Telecommunications

Cloud users are usually connected to cloud data centres via the internet. Access to cloud services is dependent on the network connectivity and speed provided by UK broadband infrastructure (POSTnote 494). In the past 5 years there has been a threefold increase in demand for video streaming from cloud-based services such as Netflix; it is estimated that cloud-enabled video streaming services will make up 80% of UK internet traffic in 2020.[30]

Security and resilience

Many organisations depend on cloud services for essential business functions (such as payroll), and the loss or compromise of these services could have significant financial consequences.[31] Many parts of the UK's critical national infrastructure; including healthcare, finance and transport; are also reliant on various cloud services.[32–34] Therefore, the security of cloud services and the data they store, and their resilience to service loss (which could be caused by cyber-attacks, power outages or CSP error) is important.[31,35–37]

Security in the cloud

Concentrating multiple users' data in a single location, or with a single CSP, may offer an attractive target for malicious actors, and outsourcing data and computation to shared data centres may expose users to cyber-attacks.[35,38–41] A 2019 survey of cybersecurity professionals found that 28% of organisations had experienced a cloud security incident between 2018–2019.[42]

Many CSPs offer a broad range of controls, cybersecurity expertise and the latest security technologies to help protect their customers.[43,44] Very few reports of CSP security failures exist.[45] However, the highly networked and distributed nature of cloud computing can render organisations vulnerable to data leaks by creating more avenues for attack.[39,42] This can be exacerbated if organisations use multiple CSPs and services.[44,46] Service models that give users more computational control, such as IaaS, require users to accept more responsibility for their security.[47] The research firm Gartner have predicted that, by 2025, 99% of cloud security incidents will be due to user errors, such as using weak passwords, falling victim to phishing attacks or misconfiguring their clouds, up from 95% in 2020.[38,48–50] Additionally, the cybersecurity firm McAfee have estimated that 99% of cloud misconfigurations go unnoticed by the organisations responsible.[51] For example, in March 2019 the US bank Capital One suffered a leak of the personal details of 100 million credit card holders after a hacker exploited a misconfiguration in one of the bank's cloud applications.[52,53]

In order to mitigate these risks, organisations need strong cloud governance policies and oversight of which cloud services they are using and where their data are stored.[43,45] The National Cyber Security Centre has produced guidelines to help organisations looking to adopt cloud services ensure that their data will be secure.[54,55] Furthermore, several cloud-specific standards have been developed that can help users compare the security of certified CSPs.[56] Users handling sensitive data often store it separately and use encryption (POSTbrief 19) to prevent malicious actors from reading it while it is transferred or stored. However, encryption services could be vulnerable to the exploitation of government mandated 'backdoors' (Box 2), though no such attacks have yet been reported.[57,58]

Cloud service resilience

It is common practice for CSPs to guarantee a minimum level of service. CSPs often have spare storage and processing capabilities to mitigate against partial capacity loss and may offer to store users' data across multiple data centres. Organisations may be able to increase their resilience by procuring services from multiple independent CSPs; however, this may increase technical complexity. In the financial services sector, cloud outsourcing is regulated by the Financial Conduct Authority to ensure operational resilience.[4,59–61]

Lock-in and interoperability

Organisations that depend on any single cloud service would be at risk if the CSP were to discontinue or alter that service. This is particularly true for PaaS users as switching to an alternative CSP may be challenging if the CSPs use different software interfaces. Users are described as being 'locked-in' to using a CSP if they are unable to move their applications to an alternative CSP without incurring significant cost or needing to rewrite their software.[62] The Government Digital Service has noted some advantages to lock-in, such as the reduction of application complexity, and has also advised that lock-in can be mitigated by developing appropriate exit strategies.[63] The EU is currently finalising codes of conduct that address cloud lock-in and clarify such exit strategies.[64,65]

Trade industry body techUK have called for the Government to encourage 'interoperability by design' so that users can write applications that will work across many different platforms and services.[84] This could mitigate lock-in risk and encourage a diverse and competitive cloud market.[84] One way this might be achieved is through an 'open standards' approach in which CSPs use the same, freely-available interface standards.[85–87]

Box 2: Cloud Legislation
This box details some of the relevant pieces of legislation affecting cloud services in the UK.

Network and Information System (NIS) Regulations
The NIS Directive was adopted by the EU in 2016 and was transposed into UK law in 2018.[66] The regulations require that digital service providers, including CSPs, take appropriate security measures to prevent actions, such as a security breach, that may compromise their stored data or services. Any such action must be reported to the Information Commissioner's Office within 72 hours.[67]

UK Investigatory Powers Act 2016 (IPA)
The IPA became UK law in 2016 and makes provisions for government interception of communications data.[68] Under this Act, communications service providers, including CSPs, may receive requests from national security services for access to customer communications.[69] This may require CSPs to create 'backdoors' in their software in order to remove protections, such as encryption, that they have applied to customers' data.[70]

UK Data Protection Act 2018 (DPA) and EU General Data Protection Regulation (GDPR)
The DPA 2018 implements requirements from the EU's GDPR in UK law. Under these laws, organisations are subject to tight controls over the collection and use of personal data.[71,72] GDPR puts primary responsibility for data protection on data controllers; those who control the means and purposes of data processing.[73] Controllers must comply with limits on the collection and retention of personal data and must allow users to move and delete their data. Data controllers may appoint data processors to process personal data on their behalf. The data processor must act only on the controller's instructions and must ensure the security of the personal data that they process.[74] Personal data can be freely transferred to a country outside of the EU if the European Commission have assessed that the country has equivalent, but not necessarily identical, privacy protections to those within GDPR.[75] Otherwise, the sender and recipient must implement appropriate contractual safeguards to ensure that the data are sufficiently protected.[75–77]

US CLOUD Act (H.R.4943)
This law clarifies that US federal law enforcement agencies can request data stored by US internet service providers (including CSPs) and their foreign subsidiaries regardless of whether the data is stored in the US or abroad.[78] CSPs can challenge these requests if there is a conflict of national laws.[79] The European Data Protection Board has given the opinion that only in very limited cases would these requests be compatible with GDPR.[80] Under the Act, the UK and US have entered into an agreement whereby law enforcement agencies of one nation may request data directly from a CSP located in the other, subject to numerous restrictions, provided that the requesting nation has jurisdiction over the CSP.[81–83]

Data and regulation

CSPs handle large quantities of data, and a single cloud service may involve multiple parties across multiple jurisdictions. For example, the music streaming service Spotify is a cloud service built on top of Google Cloud, another cloud service.[88] This means regulating data privacy, location and trade can be challenging.[43,89] The global software trade body, BSA, has listed the UK as fourth globally in regulatory preparedness for cloud adoption.[90] However, a recent survey found that 50% of UK organisations have doubts about the compliance of their cloud solutions with the range of applicable regulations.[3,4] Some UK regulations may change following the Brexit transition period.

Privacy

Cloud computing allows consumers or companies with little technical expertise to access computing resources without needing to understand the underlying technology. Cloud customers are in control of which data are put into the cloud and the purpose of data analysis, giving them primary responsibility for complying with data protection laws (Box 2). However, cloud customers may not fully understand where their data are being stored or processed. Meeting the requirements of data protection laws may prove challenging for CSPs and their customers if personal data are highly distributed across a cloud infrastructure. CSPs are subject to the privacy laws of the jurisdiction in which they operate, and sometimes these laws can have extrajudicial reach.[43,91,92]

Data residency and sovereignty

Data residency broadly describes the set of issues that relate to the location of data and its movement across jurisdictions.[43,93] For multinational CSPs, multiple copies of a user's data may be distributed across several data centres, possibly across several jurisdictions. Due to the dynamic nature of cloud, data are regularly moved. Organisations are unlikely to know the exact location of their data unless they have requested that it remains in a particular location. Some stakeholders have expressed concerns about storing data belonging to UK organisations and individuals in jurisdictions where the UK has no legal control.[94,95] The Centre for European Policy Studies has estimated that 92% of the Western world's data are stored in the United States, and 4% in Europe.[96]

Data residency regulations require that a copy of a dataset is stored within the ruling jurisdiction, whereas data sovereignty requires that a dataset can only be stored and accessed from within that jurisdiction. Residency and sovereignty allow jurisdictions to exercise greater control over their data. For example, Russia has strict data sovereignty laws that forbid external access to data about Russian citizens or Russian natural resources.[93] Others, such as Germany and France, have encouraged the establishment of sovereign clouds to comply with national data control laws.[25] The UK currently has no legal residency requirements. Documents produced by the UK, the EU and the US concerning future trade agreements have all expressed opposition to such requirements.[97–100]

Data residency requirements may increase the cost of cloud services and restrict market competition, and the resulting increase in the number of local data centres may introduce security vulnerabilities.[93,101] Residency concerns may discourage organisations from adopting cloud, and some have argued that residency requirements are an attempt to keep foreign competitors out of domestic markets.[102–105] Others, however, have argued that storing and accessing data within your own jurisdiction may have local economic advantages.[106]

Data trade after Brexit

75% of the UK's data trade is with the EU.[107] After the Brexit transition period, the continued free flow of data between UK and EU organisations, including CSPs, will be dependent on an EU assessment of the adequacy of UK privacy protections (Box 2).[101,108–110] While the UK Government has stated that it will seek to maintain "high standards", it has also stated its desire to develop independent data protection policies.[111–115]. If UK protections are not considered adequate, individual businesses would need to use EU approved safeguards in contracts involving access to EU personal data.[116] It may be particularly challenging for smaller organisations with limited legal expertise to implement these safeguards.[75,117] In order to avoid any regulatory barriers that may arise following the transition period, Google's UK users are now provisioned for by Google LLC (US), whereas previously they were under Google Ireland Ltd.[118] The UK has made specific arrangements with Japan and the US to replace EU data transfer agreements and secure the continued flow of personal data after Brexit. Negotiations with other countries are ongoing.[76,119–122]

Energy usage

Cloud computing can offer significant energy savings compared with using on-premise facilities. Modern cloud data centres make use of low power components that are optimised to run the maximum number of computing services on the minimum amount of hardware.[123–126] A recent study showed that, as a result of these efficiency gains, between 2010 and 2018 global computing output rose by 550% while energy consumption rose by only 6%.[127] Programmes such as the Climate Change Agreement for Data Centres have incentivised efficiency gains through tax breaks and energy efficiency targets.[128,129] However, Greenpeace has argued that efficiency gains in computing may lead to increased consumption overall.[130] Furthermore, the construction of new data centres in areas that have low levels of renewables in their power mixes may lead to an increased demand for fossil fuels.[130]

Barriers to technology adoption

Moving to the cloud can lead to significant changes in the way organisations manage their computing and get value from their data. Migrating large legacy IT systems to the cloud can be challenging, so some organisations may only be using the cloud for a small percentage of their workloads.[84,131,132]

A 2020 survey of public sector organisations by UKCloud found that, despite a strong desire to use cloud computing, many public sector bodies cited a lack of clear strategy, technical skills and cost management as barriers to cloud adoption.[133–135] Furthermore, the Cloud Industry Forum has reported that 50% of organisations lack the skills and knowledge needed to fully take advantage of transformative technologies such as cloud.[3]

The industry body techUK has identified seven areas where action could encourage cloud uptake, particularly among smaller enterprises.[84] These include encouraging interoperability, providing skills and guidance for organisations, improving awareness of the sustainability benefits and increasing full fibre broadband provision.

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to John Cully for researching this briefing, to the Engineering and Physical Sciences Research Council for funding his parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Susie Wright. Parliamentary Copyright 2020.

Endnotes

1. British Computing Society (2019). History of the cloud. *British Computing Society*.
2. Daley, S. (2020). COVID-19: How cloud is ready, willing and able to support home working. *techUK*.
3. Cloud Industry Forum (2018). Cloud - The Next Generation. Cloud Industry Forum.
4. Lewis, M. (2019). Cloud Computing 2020. Lexology Getting The Deal Through.
5. Government Digital Service (2017). Government Cloud First policy. *GOV.UK*.
6. Government Digital Service *et al.* (2020). Cloud guide for the public sector. *GOV.UK*.
7. techUK (2017). Cloud First: Policy not Aspiration. techUK.
8. Mell, P. *et al.* (2011). The NIST Definition of Cloud Computing. NIST.
9. Carey, S. (2020). Who rules the UK cloud market? AWS vs Azure vs Google Cloud. *Computer World*.
10. Reinsel, D. *et al.* (2018). *Data Age 2025 The Digitization of the World*. IDC.
11. Red Hat What is multicloud? *Red Hat*.
12. VansonBourne *et al.* (2019). Enterprise Cloud Index. Nutanix.
13. Watts, S. *et al.* (2019). SaaS vs PaaS vs IaaS: What's The Difference and How To Choose. *BMC Blogs*.
14. AWS Airbnb Case Study. *AWS*.
15. Costello, K. *et al.* (2019). Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018. *Gartner*.
16. Canalys (2020). Cloud market share Q4 2019 and full-year 2019. *Canalys*.
17. Synergy Research Group (2019). Amazon, Microsoft, Google and Alibaba Strengthen their Grip on the Public Cloud Market. *Synergy Research Group*.
18. Synergy Research Group (2019). SaaS Spending Hits $100 billion Annual Run Rate; Microsoft Extends its Leadership. *Synergy Research Group*.
19. Crown Commercial Service *et al.* Digital Marketplace: Cloud hosting, software and support. *GOV.UK*.
20. du Preez, D. (2019). Did the government kill off the Oligopoly or just send it back to the (US) cloud? *Diginomica*.
21. de Quetteville, H. (2019). Special report: Amazon's extraordinary grip on British data. *The Telegraph*.
22. Donnelly, C. (2018). Assessing the hyperscale squeeze on G-Cloud's SMEs. *Computer Weekly*.
23. James, M. (2020). Digital sovereignty: Time for Britain to take back control of our data. *City A.M.*
24. Hansford, S. (2020). A National Asset: Why Data (Sovereignty) is Vital for UK Citizens. *Computer Business Review*.
25. Federal Ministry for Economic Affairs and Energy *et al.* Project GAIA-X. Federal Ministry for Economic Affairs and Energy.
26. European Commission (2020). A European strategy for data. European Commission.
27. Bedingfield, W. (2020). Europe has a plan to break Google and Amazon's cloud dominance. *Wired UK*.
28. AWS Six Advantages of Cloud Computing - Overview of Amazon Web Services.
29. Intellect (2013). Er, what IS a data centre? techUK.
30. Cisco (2016). United Kingdom - 2020 Forecast Highlights. Cisco.
31. Uptime Institute (2019). 2019 Annual Data Center Survey Results. Uptime Institute.
32. NHS Digital (2018). NHS and social care data: off-shoring and the use of public cloud services. *NHS Digital*.
33. Palmer, M. (2019). On the road to digital transformation with UK's Department for Transport. *Google Cloud*.
34. European Banking Authority (2018). EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech. European Banking Authority.
35. McCarthy, K. (2019). Amazon is saying nothing about the DDoS attack that took down AWS, but others are. *The Register*.
36. Kunert, P. (2011). Lightning strikes cloud: Amazon, MS downed. *The Register*.
37. Sverdlik, Y. (2017). AWS Outage that Broke the Internet Caused by Mistyped Command. *Data Centre Knowledge*.
38. Oracle *et al.* (2019). Oracle and KPMG Cloud Threat Report 2019. Oracle.
39. Verizon (2019). *2019 Data Breach Investigations Report*. Verizon.
40. Metivier, B. (2019). The Concentration Risk of Cloud Services. *Sage Advice - Cybersecurity Blog*.
41. Andrew A (2018). My cloud isn't a castle. *National Cyber Security Centre*.
42. Cybersecurity Insiders (2019). 2019 Cloud Security Report. Cybersecurity Insiders.
43. Rashid, A. *et al.* (2019). The Cyber Security Body of Knowledge. University of Bristol.
44. Nominet (2019). Cyber security and the cloud. Nominet Cyber Security.
45. Heiser, J. (2018). Clouds Are Secure: Are You Using Them Securely? Gartner.
46. March, T. *et al.* (2020). NCSC explores potential security opportunities that can come with using the GDS cloud lock-in guidance. *GOV.UK*.
47. Microsoft (2019). Shared responsibility in the cloud. *Microsoft*.
48. Panetta, K. (2019). Is the Cloud Secure? *Gartner*.
49. Check Point (2020). Cyber Security Report 2020. 80. Check Point.
50. Pettey, C. (2016). Why Cloud Security Is Everyone's Business. *Gartner*.
51. McAfee (2019). Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report. McAfee.
52. Murphy, H. *et al.* (2019). Capital One data breach sparks cloud security fears. *Financial Times*.
53. Nigel C (2019). There's a hole in my bucket. *National Cyber Security Centre*.
54. National Cyber Security Centre (2018). Cloud security guidance. *National Cyber Security Centre*.
55. National Cyber Security Centre (2019). NCSC CAF guidance. *National Cyber Security Centre*.
56. Cloud Standards Customer Council (2016). Cloud Security Standards: What to Expect & What to Negotiate Version 2.0. Object Management Group.
57. Ashford, W. (2019). Security pros reiterate warning against encryption backdoors. *Computer Weekly*.
58. Malwarebytes What is a backdoor? *Malwarebytes*.
59. Bank of England *et al.* (2018). Building the UK financial sector's operational resilience. Bank of England.
60. Financial Conduct Authority (2019). FG16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services. Financial Conduct Authority.
61. British Bankers' Association *et al.* (2016). Banking on Cloud A discussion paper by the BBA and Pinsent Masons. British Bankers' Association.
62. Cloud Flare What Is Vendor Lock-In? | Vendor Lock-In and Cloud Computing. *Cloud Flare*.
63. Government Digital Service (2019). Managing technical lock-in in the cloud. *GOV.UK*.
64. Cloud and Software (Unit E.2) (2019). Presentation of Codes of Conduct on cloud switching and data portability. *European Commission*.
65. SWIPO Working Group (2019). Multi-stakeholder group presents Codes of Conduct to enable competition and data

portability for cloud service customers across Europe. *European Commision*.
66. The Network and Information Systems Regulations 2018.
67. Information Commissioner's Office The Guide to NIS. *Information Commissioner's Office*.
68. Investigatory Powers Act 2016.
69. Smith, G. (2016). The UK Investigatory Powers Act 2016 – what it will mean for your business. *Bird & Bird*.
70. Carey, S. (2019). The Snoopers' Charter: Everything you need to know about the Investigatory Powers Act. *Computer World*.
71. Data Protection Act 2018.
72. Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR). *Information Commissioner's Office*.
73. Gabel, D. *et al.* (2019). Chapter 10: Obligations of controllers – Unlocking the EU General Data Protection Regulation. *White & Case*.
74. Gabel, D. *et al.* (2019). Chapter 11: Obligations of processors – Unlocking the EU General Data Protection Regulation. *White & Case*.
75. techUK *et al.* (2017). No interruptions: Options for the future UK-EU data-sharing relationship. techUK.
76. Information Commissioner's Office International data transfers. *Information Commissioner's Office*.
77. Ross, N. (2019). Explaining adequacy; personal data transfers to the EEA under no deal. *techUK*.
78. US Cloud Act 2018.
79. Smith, B. (2018). The CLOUD Act is an important step forward, but now more steps need to follow. *Microsoft*.
80. Jelinek, A. *et al.* (2019). LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection.
81. Foreign & Commonwealth Office (2019). UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019].
82. Crime (Overseas Production Orders) Act 2019.
83. Anderson, T. *et al.* (2019). U.S. and U.K. Sign CLOUD Act Agreement. *Inside Privacy*.
84. techUK (2019). Cloud 2020 and beyond. techUK.
85. Cabinet Office (2018). Open Standards principles. *GOV.UK*.
86. IBM (2015). Cloud standards: Tools to ensure cloud application interoperability. *IBM*.
87. Openforum Europe (2017). ICT Standardisation in a Digital world. Openforum Europe.
88. Google Cloud Spotify: The future of audio. Putting data to work, one listener at a time. *Google Cloud*.
89. Organisation for Economic Co-operation and Development (2014). Cloud Computing: The Concept, Impacts and the Role of Government Policy. Organisation for Economic Co-operation and Development.
90. Galexia (2018). 2018 BSA Global Cloud Computing Scorecard. BSA The Software Alliance.
91. IT Pro (2019). GDPR and the cloud. *IT Pro*.
92. Tolsma, A. GDPR and the impact on cloud computing. *Deloitte*.
93. Cloud Standards Customer Council (2017). Data Residency Challenges, A Joint Paper with the Object Management Group. Object Management Group.
94. BBC (2018). NHS Digital approves data off-shoring in new guidance. *BBC News*.
95. Winder, D. (2018). Cloud still hangs over patient data sovereignty concerns. *Digital Health*.
96. Kalff, D. *et al.* (2020). Hidden Treasures: Mapping Europe's sources of competitive advantage in doing business. Centre for European Policy Studies.
97. Prime Minister's Office (2020). DRAFT UK-EU Comprehensive Free Trade Agreement (CFTA). Prime Minister's Office.
98. European Commission (2020). Draft text of the Agreement on the New Partnership with the United Kingdom. European Commission.
99. Department for International Trade (2020). The UK's approach to trade negotiations with the US. Department for International Trade.
100. Office of the United States Trade Representative (2019). United States-United Kingdom Negotiations Summary of Specific Negotiating Objectives. Office of the United States Trade Representative.
101. Wickham Heath Consulting (2018). Cross-Border Data Flows Realising benefits and removing barriers. GSMA.
102. Manancourt, V. (2020). Europe's data grab. *Politico*.
103. Bauer, M. *et al.* (2016). Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization. Centre for International Governance Innovation.
104. Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology & Innovation Foundation.
105. Beattie, A. (2018). Data protectionism: the growing menace to global business. *Financial Times*.
106. Hicks, J. (2019). 'Digital colonialism': why some countries want to take control of their people's data from Big Tech. *The Conversation*.
107. Frontier Economics (2017). The UK Digital Sector After Brexit. techUK.
108. Ferracane, M. (2017). Restrictions on Cross-Border Data Flows: A Taxonomy. *SSRN Electronic Journal*,
109. Organisation for Economic Co-operation and Development (2019). Trade and Cross-Border Data Flows. Organisation for Economic Co-operation and Development.
110. Ross, N. (2020). Data, adequacy and the future relationship – an explainer. *techUK*.
111. Johnson, B. (2020). UK / EU relations: Written statement - HCWS86.
112. DCMS (2020). Explanatory framework for adequacy discussions. *GOV.UK*.
113. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.
114. Woodhouse, J. *et al.* (2017). Brexit and data protection. House of Commons Library.
115. Lloyd, L. (2020). UK–EU future relationship: data adequacy. *Institute for Government*.
116. ICO (2020). Keep data flowing from the EEA to the UK – interactive tool.
117. Patel, O. *et al.* (2019). EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray? *SSRN Electronic Journal*,
118. Menn, J. (2020). Exclusive: Google users in UK to lose EU data protection - sources. *Reuters*.
119. US Department of Commerce (2020). Privacy Shield and the UK FAQs. *Privacy Shield Framework*.
120. European Commission Adequacy decisions. *European Commission*.
121. European Commission (2019). EU-US data transfers. *European Commission*.
122. European Data Protection Supervisor International Agreements. *European Data Protection Supervisor*.
123. Jones, N. (2018). How to stop data centres from gobbling up the world's electricity. *Nature*, Vol 561, 163–166.
124. Open Compute Project. *Open Compute Project*.
125. The Green Grid. *The Green Grid*.
126. UKCloud (2016). Greening Government ICT: How cloud can help. UKCloud.
127. Masanet, E. *et al.* (2020). Recalibrating global data center energy-use estimates. *Science*, Vol 367, 984–986.

128. techUK Climate Change Agreement (CCA) for Data Centres Target Period One: Report on findings. techUK.
129. European Energy Efficiency Platform (2016). Code of Conduct for Energy Efficiency in Data Centres. *European Commision*.
130. Greenpeace (2017). Clicking Clean: Who is Winning the Race to Build a Green Internet? 102. Greenpeace.
131. Lawrence, A. *et al.* (2019). Enterprise IT and the public cloud: What the numbers tell us. *Uptime Institute*.
132. Government Digital Service (2019). Managing legacy technology. *GOV.UK*.
133. UKCloud (2020). State of Cloud Adoption UK Public Sector Survey Report 2020. UKCloud.
134. Government Digital Service (2020). Managing your spending in the cloud. *GOV.UK*.
135. Government Digital Service (2020). Creating and implementing a cloud hosting strategy. *GOV.UK*.