PART I

Subject Matter

1

Introduction

Cloud computing has been promoted as a significant development in information and communications technology (ICT) outsourcing. At its core, cloud computing is a method of providing users with on-demand computing services, generally delivered over the Internet.[1] Cloud computing provides users with data storage, use of software and an array of applications.[2] Combined with improving networks and Internet access, cloud computing makes it possible for users to migrate their data using remote servers and infrastructure owned by third parties.[3] Simply stated, paperwork that in the past was digitalized and moved from the filing cabinet to the personal computer has now moved farther to server parks located around the globe. Worldwide access to documents, innovative services, improved data administration, and advanced security make adopting cloud computing an attractive proposition for many users including governments.

This movement, from local storage to central storage accessed over the Internet, has fundamentally changed the way users interact with their data. With the help of cloud computing, ubiquitous computing has now become a reality.[4] Data is essentially available anywhere at any time and is accessible on multiple devices. Even if the technologies behind it are not new, cloud computing is often billed as the future of computing and has a central place in corporate and governmental ICT strategies.

Providing that cloud computing systems function properly, they have generally not been of interest to the public. However, revelations of access to data by security services and law enforcement agencies(LEAs), data security concerns (including data breaches and data ransom), data loss, and profiling of users by private

[1] Christopher S. Yoo, 'The Changing Patterns of Internet Usage' (2010) 63 *Federal Communications Law Journal* 67–90 at 83.

[2] See Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing' (2011) *Special Publicaion (NIST SP) 800–145*. https://csrc.nist.gov/publications/detail/sp/800-145/final.

[3] William Jeremy Robison, 'Free at What Cost?: Cloud Computing Privacy under the Stored Communications Act' (2010) 98 *Georgetown Law Journal* 1195–239 at 1198.

[4] Tobias Matzner, 'Why Privacy is Not Enough Privacy in the Context of "Ubiquitous Computing" and "Big Data"' (2014) 12 *Journal of Information, Communication and Ethics in Society* 93–106 at 93. Ubiquitous or 'pervasive' computing refers to computing power that is essentially everywhere.

companies for commercial purposes have all drawn attention to the use of cloud computing.[5] Issues related to cloud computing have been central in cases before both the US Supreme Court and the Court of Justice of the European Union(EU).

The perceived lack of control over data stored on the cloud from either a physical or logical perspective has limited uptake of cloud computing.[6] This is particularly the case in regulated and governmental sectors. In other words, broader adoption of cloud computing by the public sector remains overcast in many areas. The reality of the situation is that the central barriers or bottlenecks to broader cloud adoption are no longer technical problems, but rather legal ones. Therefore, the aim of this book is to analyse the core legal issues that are central to government adoption of cloud computing services.

1.1 GOVERNMENT CLOUD COMPUTING IN CONTEXT

Governments spend substantial amounts of money on their information technology (IT) systems.[7] For instance, in the United States, the president's fiscal year 2019 budget request for IT was more than $90 billion.[8] Although IT systems generally increase government efficiency in delivering services to citizens, when computing systems grow in complexity they demand greater technical competence and become increasingly expensive to operate and maintain.[9] Numerous governments have focused on cloud computing as an important tool for providing state-of-the-art IT at a lower cost. Cloud computing allows governments to obtain computing power on a pay-per-use basis and removes many of the limits that governments have in developing new systems or applications in-house, allowing IT departments to focus on areas critical to their administration. Cloud computing also offers flexibility and a lower cost of ownership than many IT outsourcing services.

Although cloud computing may overcome some challenges and reduce computing expenses, certain aspects of the technology and its deployment raise additional concerns. For example, the cloud service provider's (CSP's) infrastructure is often

[5] *American Broadcasting Co., Inc.* v. *Aereo, Inc.* [2014] 134 S. Ct. 2498. Evaluating the application of copyright laws to new technologies, such as cloud computing. Cheng Lim Saw and Warren B. Chik, 'Whither the Future of Internet Streaming and Time-shifting? Revisiting the Rights of Reproduction and Communication to the Public in Copyright Law after Aereo' (2015) 23 *International Journal of Law and Information Technology* 53–88 at 84.

[6] Rania El-Gazzar, Eli Hustad, and Dag H. Olsen, 'Understanding Cloud Computing Adoption Issues: A Delphi Study Approach' (2016) 118 *Journal of Systems and Software* 64–84 at 73. Finding that global data privacy compliance was among top concerns of cloud clients. W. K. Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens* (Cheltenham and Northampton, MA: Edward Elgar 2017), p. 274. Evaluating the differences between logical and physical security.

[7] David A. Powner et al., United States Government Accountability Office (GAO), 'Information Technology: Federal Agencies Need to Address Aging Legacy Systems' (Report 11 June 2019). www.gao.gov/assets/700/699616.pdf.

[8] ibid.

[9] ibid.

opaque, located on a global scale, and spread across many providers. The full extent of the cloud service may not be fully visible to the user. Moving IT services outside of an organization's physical boundaries means lost or reduced control over data and greater reliance on third parties.[10] Rather than the user making key decisions on central information management issues, such as the physical location of the infrastructure, use of subcontractors, and security methods, these aspects are typically determined by the CSP. As a result, users of cloud services (cloud clients) face many difficult questions regarding legal requirements, trust, reliability, and overall security, in addition to technical challenges, such as migration from legacy systems and interoperability.[11]

These factors potentially expose governments to additional security and privacy risks. Further increasing these risks in many cloud models is the delivery of the services over a multi-tenant infrastructure, which involves sharing resources with unknown users. Moreover, controls commonly used or available in traditional IT hosting to meet information security, confidentiality, and privacy requirements – including on-site audits, staff interviews, and individualized nondisclosure agreements – may be unavailable in the cloud computing environment.[12] As a result of the standard structure, users are often required to accept greater – or different – levels of risk than they would under traditional IT outsourcing arrangements. For governments, the level of risk they are required to bear may be too high as the tools they generally employ for mitigating risks are unavailable (e.g. audits of CSPs and subcontractors).

In addition to general security or availability concerns, cloud computing brings with it many compliance challenges affecting data privacy, law enforcement investigations, and even state sovereignty. For example, as cloud users increasingly store important documents and sensitive data on remote servers owned by third parties, questions regarding who has access to that information are becoming more important. From a commercial perspective, theft of critical business information or industrial espionage is a serious threat to the profitability and longevity of commercial enterprises. From the perspective of governments, access by foreign governments to critical state information is a threat to national security.[13] Although much of the discussion on these issues in the media has focused on the US government covertly

[10] Wayne Jansen and Timothy Grance, 'Guidelines on Security and Privacy in Public Cloud Computing' (2011) *SP 800–144*, 12. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

[11] David C. Wyld, 'Moving to the Cloud: An Introduction to Cloud Computing in Government' (2009) *IBM Center for the Business of Government*, 33. www.businessofgovernment.org/sites/default/files/CloudComputingReport.pdf.

[12] See generally Scott Paquette, Paul T. Jaeger, and Susan C. Wilson, 'Identifying the Security Risks Associated with Governmental Use of Cloud Computing' (2010) 27 *Government Information Quarterly* 245–53 at 248.

[13] Norwegian Ministry of Local Government and Modernisation, 'Cloud Computing Strategy for Norway' (2016) *Publication number H-2365 E*, 11. www.regjeringen.no/en/dokumenter/cloud-computing-strategy-for-norway/id2484403/.

accessing sensitive information, access concerns extend beyond the US government to include not only other governments but private parties as well.[14]

The aforementioned risks impact many cloud computing users. However, in addition to the reservations held by private businesses or consumers, governments have additional concerns. From a practical perspective, in addition to highly regulated purchasing regimes, government users are often subject to publicly mandated computing security and archive requirements.[15] Unlike the private sector, governments cannot deviate from these requirements. Some of these requirements pose a direct barrier to adopting cloud, while others simply make cloud computing less attractive than more traditional IT outsourcing arrangements.

Governments represent citizens who are the beneficiaries of potential monetary savings from cloud services, but also bear the burden of government oversights in the procurement and operation of those services. Taking into account their position of trust and responsibility to the public, governments are generally required to exercise a higher level of transparency and accountability than private businesses or consumers when contracting for their own computing needs. Similarly, concerns regarding control, sometimes expressed as sovereignty, over data are particularly acute when considering the role of the state. If the state were to lose control over its data, there would be significant consequences for its ability to govern.

An additional concern for governments is that the portfolio or types of data they have are often extremely sensitive. For example, a government may hold census data, tax records, health data, records of criminal offences, and employment and education records, among other data types, on any of its citizens. Furthermore, citizens have little choice but to submit such data to the state in order to obtain services or comply with the law. In other words, although individuals can at least arguably opt out of using services like Google or Facebook, they cannot opt out of paying their taxes. The result is that the data possessed by governments on their citizens is multifaceted, sensitive, and devoid of active or direct consent on the part of the citizen.

In order to offer a standard or an interchangeable service, CSPs tend to provide their contract terms on a standard basis.[16] For governments, the contract terms contained in these offers are often unacceptable as they fail to account for their somewhat unique legal and security requirements. To counter this reality, governments with broader cloud procurement strategies often require CSPs to adhere to specific contract terms or even require that CSPs offer their services based on a contract that is essentially drafted by the government. In theory, central governments have enough negotiating power that they are able to force CSPs to the

[14] Fred H. Cate and others, 'Systematic Government Access to Private-sector Data' (2012) 2 *International Data Privacy Law* 195–99 at 196.

[15] See generally the Federal Information Security Management Act of 2002 ('FISMA') 44 USC § 3541 (2002) and the Federal Information Security Management Act of 2002, Pub. L. No. 107–347 (2002).

[16] Kristina Irion, 'Your Digital Home is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship between Individuals and Their Personal Records' (2015) 23 *International Journal of Law and Information Technology* 348–71 at 358–59.

bargaining table and move past the incompatible 'take it or leave it' contract terms faced by consumers and small- and medium-sized enterprises (SMEs).

The question remains: do current approaches to procuring cloud services meet the legal requirements of governments? Do legal requirements amount to traversable roadblocks or dead ends? In other words, are the terms or templates used in cloud procurement programs sufficient to allow governments to meet their legal and security requirements in light of data protection and other applicable laws and regulations? In evaluating these issues, the book focuses on the legal requirements, such as application of the General Data Protection Regulation (GDPR) and specific procurement or contracting requirements, and their application to cloud computing. In the subsequent chapters I assess whether these sources provide legal constraints that limit cloud computing as a viable means of computing for many governments.

1.2 MEETING LEGAL REQUIREMENTS: PROCUREMENT PLANS, CONTRACTS

In the absence of legislation that addresses the challenges of cloud computing, contracts play a central role in filling the gaps. Whether they have accomplished this objective and what legal implications these agreements have for users are ongoing questions. A primary challenge in this regard is that contracts drafted for globally accessible cloud services are still subject to national speed limits in many respects. The current approach to meeting legal requirements for most governments is utilizing contractual means rather than technical ones. That is, rather than building cloud computing systems and becoming CSPs themselves, governments focus on procurement strategies for contracting with private providers.

To provide a better understanding of how these procurement plans work and how they meet data privacy and other legal requirements, I examine the contracting tools of two of the largest and most developed systems currently in use, namely the Government Cloud (G-Cloud) system in the United Kingdom and the Federal Risk and Authorization Management Program (FedRAMP) system in the United States.[17] Much of the contractual analysis is based on an evaluation of the actual content of contracts between US federal agencies and CSPs obtained through the Freedom of Information Act (FOIA) disclosures from the US government.[18] I also evaluate standard agreements offered as part of the United Kingdom's G-Cloud

[17] The United Kingdom was selected for the FOIA study and research generally *prior to* invoking Article 50 of the Treaty on European Union and staring the withdrawal process known as 'Brexit'. The process was not complete by the time this book was finalized. See generally European Commission, 'Negotiating Documents on Article 50 Negotiations with the United Kingdom'. https://ec.europa.eu/commission/brexit-negotiations/negotiating-documents-article-50-negotiations-united-kingdom_en.

[18] The Freedom of Information Act 5 USC § 552, As Amended by Pub. L. No. 104–231, 110 Stat. 3048 (hereinafter 'FOIA'). www.justice.gov/oip/blog/foia-update-freedom-information-act-5-usc-sect-552-amended-public-law-no-104-231-110-stat.

framework in addition to cloud contracts obtained under the UK Freedom of Information Act (UK FOIA) available in the public sphere.

After evaluating legal requirements and governmental plans to meet those requirements, the question then becomes whether there is a compliance gap between what the procurement systems require and what the contracts actually contain. If such a gap exists, what are the potential problems or risks created for citizen and government data? Have government agencies or actors adequately protected the privacy interests of the citizens they represent? If there are gaps between what the FedRAMP system requires and what was procured, are European systems, including the United Kingdom's G-Cloud system, in a better position to prevent these oversights? In other words, if the G-Cloud system had been applied by US agencies, would they have obtained a more compliant or better result? The main objective of this comparison is to determine which requirements led to the best results when applied to the cloud structure.

In addition to specific applicable laws and the contracts designed to act in accordance with those laws, I consider whether governments should be concerned with the centralizing of data that takes place through cloud usage and its potential impact on data sovereignty. In other words, is the creation of centralized storage points, with the massive amounts of critical data stored and managed by private providers, a systemic concern that goes beyond security breaches and other periodic security lapses for governments?[19] If so, how should governments approach these risks?

1.3 IMPACT AND SCOPE

When legal literature on cloud computing first began to be published, there was a considerable focus on whether cloud computing amounted to anything more than a clever marketing term.[20] That debate has now been settled in most circles. Most researchers seem to acknowledge that cloud computing services go one step further, or take a different direction, than those offered or employed in traditional IT hosting or outsourcing arrangements.[21] However, the question remains: how are cloud services best regulated? Should private ordering – including private contracts between parties – retain its primacy in governance or should governments on a top-down basis set more cloud-specific regulations?[22]

[19] David Lametti, 'The Cloud: Boundless Digital Potential or Enclosure 3.0?' (2012) 17 *Virginia Journal of Law & Technology* 192–243 at 214.

[20] Damon C. Andrews and John M. Newman, 'Personal Jurisdiction and Choice of Law in the Cloud' (2013) 73 *Maryland Law Review* 313–84 at 313. Stating that '[t]hough some early detractors criticized the "cloud" as being nothing more than an empty industry buzzword, we contend that by dovetailing communications and calculating processes for the first time in history, cloud computing is – both practically and legally – a shift in prevailing paradigms'.

[21] ibid., 325. Arguing that cloud computing is more than a 'buzzword'.

[22] Anthony Gray, 'Conflict of Laws and the Cloud' (2013) 29 *Computer Law & Security Review* 58–65 at 64. See Chapter 4, evaluating examples of direct legislation in the 'Clarifying Lawful Overseas Use of Data Act (CLOUD Act)'.

As 'cloud clients', governments have great potential to influence the cloud computing market. As noted by Marsden,

> Government, it is often forgotten, does far more to regulate than simply tax and spend, legislate, rule-make and prosecute. It is also the largest procurer of goods and services, the first adopter of many new technologies, and the commissioner of most new basic research, especially in Europe.[23]

For example, as the largest buyer of cloud computing services worldwide, the US government influences how cloud computing develops through both its purchasing power and its legislation.[24] Even if the EU currently lags behind the United States in terms of cloud usage and adoption, the EU has one of the largest potential markets of active Internet users. EU laws and initiatives will shape the future of cloud by either limiting or embracing its adoption in much of the public sector and beyond.[25]

Although this book primarily considers the role of governments as users or adopters of cloud computing, states are also taking on additional roles. Governments also act as contributors to cloud computing research, standards development and as market regulators. For example, by developing model contract terms and playing an active part in the development of certification schemes, governments play an important role in influencing the private ordering that is used to largely regulate cloud computing. If states can effect changes in the way CSPs deliver services, making them more compliant with data privacy laws, then these changes may also trickle down to consumer and business deployments.

1.4 DEFINITIONS, CONCEPTS, AND PARAMETERS

1.4.1 *Article 29 Working Party (WP29) and the European Data Protection Board (EDPB)*

Article 29 of the EU Data Protection Directive specifically established a working party to provide guidance on data protection law in the EU (henceforth WP29). The WP29 had an advisory role and was comprised of one representative from each of the data protection authorities (DPAs) in the EU member states, the European Data Protection Supervisor (EDPS), and the European Commission. At the EU level,

[23] Christopher T. Marsden, 'An Empire Entire of Itself? Standards, Domain Names and Government' in Christopher T. Marsden (ed.), *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge: Cambridge University Press 2011), p. 101.

[24] Government Accountability Office (GAO), 'Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance' (2016) GAO-16–325, 3. www.gao.gov/products/GAO-16-325. Estimating that the US federal government spent $2 billion on cloud computing services annually in addition to over $80 billion on IT generally.

[25] European Union Agency for Network and Information Security (ENISA), 'Good Practice Guide for Securely Deploying Governmental Clouds' (2013), 1. www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds.

although non-binding, opinions and guidance by the WP29 have been particularly influential.[26]

With the adoption of the GDPR on 25 May 2018, the WP29 was disbanded. The EDPB has replaced it.[27] This board is an independent European body charged with providing consistent application of the GDPR throughout the EU and facilitating cooperation with national DPAs. The EDPB is similar to the WP29 in make-up; however, the EDPB has the authority to make binding decisions in some instances.[28] After succeeding the WP29, the EDPB adopted GDPR-relevant WP29 guidelines from 2016 until 2018.[29] To avoid confusion, I use WP29 to refer to decisions made under that regime and EDPB to refer to decisions made by the DPA envisioned under the GDPR.

1.4.2 *Cloud Computing*

Cloud computing is not a new technology, but rather a combination of numerous technologies that have allowed providers to deliver computing power as a service over the Internet.[30] Although this definition is further explored in Chapter 2, I use the terms 'cloud computing service', 'the cloud', and 'cloud' to refer to the delivery of a computing service not a new technology or physical place.[31] Simply stated, cloud computing offers a means of providing users with on-demand computing services over a network. The classification of cloud computing by the National Institute of Standards and Technology (NIST) has been widely accepted in the United States and Europe and is the primary definition used in this book. The NIST definition states:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[32]

[26] WP29 was set up under the EU Data Protection Directive 95/46/EC at Art. 29. Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press 2014), p. 19.

[27] GDPR Arts. 63–76 and Recitals 135–40.

[28] EDPB, 'European Data Protection Board Rules of Procedure' (25 May 2018), 6–11. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop_adopted_en.pdf. EDPB is composed of the head of each DPA and the EDPS. The European Commission has participation but no voting rights.

[29] See EDPB, 'Endorsement 1/2018' (25 May 2018). https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf. Guidelines adopted by the EDPB primarily focus on the GDPR.

[30] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books 2006), p. 144. There are additional theories on the layers of the Internet. See generally Lawrence B. Solum and Minn Chung, 'The Layers Principle: Internet Architecture and the Law' (2004) 79 *Notre Dame Law Review* 815–948 at 816.

[31] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (henceforth 'NIS Directive') Recital 17. Providing that resources that make up cloud computing include 'networks, servers or other infrastructure, storage, applications and services'.

[32] Mell and Grance, 'The NIST Definition of Cloud Computing', 2. Dimitra Liveri and M. A. C. Dekker, 'Security Framework for Governmental Clouds: All Steps from Design to