Introduction: a walk in the clouds

Anne S.Y. Cheung and Rolf H. Weber

Cloud computing is fast becoming an integral part of daily life, with people’s activities in the physical world or on personal computers increasingly moving to web-based services ‘up in the cloud’. The cloud allows us to access our documents, photos, and video files from anywhere in the world. Many of us are customers of Dropbox and Google, amongst other cloud service providers. Be it online searching, media streaming or WhatsApping, we are all in the cloud. In addition, many businesses have purchased computing resources through cloud service providers rather than acquiring their own physical IT assets. The ubiquity of the cloud is also attracting considerable research attention, with researchers from academic and research institutions carrying out investigations into various aspects of cloud computing, from ensuring the efficient and effective use of such computing to infrastructure issues, cloud service models and cloud security. Leading IT analyst firm Gartner claims that by 2016, cloud computing will account for the bulk of all new IT spending, whereas consulting firm McKinsey estimates that the total annual economic impact of cloud technology could reach US$6.2 trillion by 2025. Furthermore, according to McKinsey, most of that impact ($1.2–5.5 trillion) could take the form of the additional surplus


3 James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson and Alex Marrs, ‘Disruptive Technologies: Advances that Will Transform
Privacy and legal issues in cloud computing

generated by the cloud delivery of services and applications to Internet users, with the remainder resulting from the use of cloud technology to improve enterprise IT productivity.\footnote{Ibid.} In other words, ‘cloud’ is no longer a mere buzzword for cool technology, but rather represents a significant paradigm shift in technological advancement and our daily lives.

Whilst cloud computing is providing us with unprecedented convenience, and thus unleashing commercial and social innovation, it has also led to great uncertainty concerning a multitude of individual rights, such as the right to privacy, security and intellectual property, particularly because of its reliance on cross-border data hosting and outsourcing. This book discusses and analyses various approaches to addressing these problems, in particular issues pertaining to security, personal data protection, contracting and licensing, jurisdiction, regulatory framework reform and content regulation. It also looks at the specific implications for cloud computing, information ownership, geographic management and biomedical practice. The major jurisdictions studied are the United States and the European Union.

Most cloud companies are techno giants based in the US (including Google and Amazon), whilst the European Union takes pride in its privacy protection regime.\footnote{Mark Scott, ‘European Firms Turn Privacy into Sales Pitch’ (NYTimes Bits Blog, 11 June 2014), http://bits.blogs.nytimes.com/2014/06/11/european-firms-turn-privacy-into-sales-pitch/?_php=true&__type=blogs&_php=true&__type=blogs&_r=2, accessed 9 August 2014.} Given the rise of global data flows, this situation has triggered intriguing dynamics, not only for the companies and cloud users in those two jurisdictions but also for those in other areas. Individual chapters discuss the implications of cloud computing in Belgium, Australia, the UK, China and Hong Kong.

Containing the forces of technology within the existing legal landscape has long constituted an uphill battle. Computer scientists are always one step ahead of the barely imaginable and thinking ahead to the next generation of tools and gadgets that will change the world as soon as technology catches up with innovation. Whilst the law does not wish to act so quickly that it stifles innovation, it also does not want to lag so far behind as to be useless. In joining the battle over how law and policy can appropriately tackle the challenges of cloud computing, this book brings together international experts from academe (legal and computer science) and industry, as well as legal professionals and representatives of the
regulatory authorities, to explore the complex legal and privacy challenges brought about by rapidly evolving cloud computing technology.

The opening chapter (by Joe Kong, Xiaoxi Fan and K.P. Chow) takes up the subject of cloud computing by providing a basic introduction to the latest agreed definition of cloud computing, its corresponding models and its various deployment methods. Moreover, it gives an overview of the information security and privacy issues related to cloud computing, and offers a hybrid legal-technological solution. Contrary to common belief, encryption is not a silver bullet to resolving personal data privacy and security problems. Accordingly, the authors discuss the advantages and disadvantages of various encryption technologies. Regardless of how much companies invest in information security enhancement, incidents of malicious system attacks, accidental data loss and deletion are still worryingly common. Kong and his team argue that personal data privacy and data security are the responsibility of both cloud service providers and users.

Chapters 2 and 3 turn their attention to the regulatory challenges posed by cloud computing. In Chapter 2, Henry Chang examines these challenges primarily from the perspective of data protection authorities (DPAs). The diverse nature of cloud markets and the complex offerings of cloud service providers in each, create considerable challenges for DPAs when it comes to the protection of personal data stored in the cloud. As a cloud service can be considered a special form of outsourced service, this chapter begins with a general description of the data protection challenges that arise when outsourcers are used to store and/or process personal data. It then goes on to analyze the three cloud-related issues that raise the greatest concerns amongst organizational users, including issues of cross-border data transfer between jurisdictions, the loose subcontracting arrangements entered into by cloud service providers, and the standard terms and conditions they offer. Chang also assesses the advice given by DPAs to both organizational users and consumers around the world on the use of cloud computing.

Sticking to the theme of regulatory challenges, Rolf H. Weber in Chapter 3 concentrates on examining the available regulatory instruments for cloud computing, namely the ex ante concept of sector-specific regulation and the dimensions of ex post competition law. In doing so, he places emphasis on the problems associated with imprecise EU legislation affecting cloud computing growth and the concept of ‘net neutrality’. Furthermore, the chapter addresses the risks of vertical integration, that is, contractual relations between an Internet service provider and a cloud provider leading to subsequent discrimination against other providers. To
further foster the growth of cloud computing, Weber argues that introducing sector-specific regulation constitutes the most sensible choice, as it would allow a more determinative assessment of a party’s rights and obligations.

In the midst of our examination of cloud-related privacy, security and regulatory concerns, Anne Cheung in Chapter 4 asks the fundamental question of what personal data is and what it should be. The current definition of personal data in most jurisdictions often hinges on whether the data can be linked to an identifiable or identified person. However, with the ongoing advancement and growing use of re-identification technology, coupled with the huge amount of data being processed and stored in the cloud across the globe, data can be easily ‘re-personalized’. This situation leads to the next logical question, which is whether anonymous, anonymized, pseudonymous or fragmented data can or should be considered personal data. The implications for the process and storage of such data in the cloud and the sale of consumer and health data cannot be underestimated. Thus, Cheung argues that a more nuanced definition and understanding of personal information/data is needed. In analyzing the current US approach and the proposed EU Data Protection Regulation, she further argues that a harmonized definition that factors in harm and risk, predictability, and flexibility in the shifting technological landscape should be formulated.

Chapters 5 and 6 confront the thorny issues of cross-border data flows and jurisdiction that crop up in any discussion of the Internet and the cloud. In Chapter 5, Dominic Staiger addresses the challenges created through cross-border data transfers on the cloud from the EU to the US, and reviews the legal response to these challenges under the current EU Data Protection Directive and the proposed EU Data Protection Regulation. In particular, he highlights issues related to the inadequacies of the Safe Harbor framework and the definitional ambiguities in the proposed EU regulation. The chapter further analyses the effects of such ambiguities and inadequacies on the actors involved in different cloud service types and scenarios, and discusses the key points that these actors should keep in mind.

Jean-Philippe Moiny in Chapter 6 defines the concept of jurisdiction, and illustrates the many jurisdictional conflicts that occur in attempting to regulate the cloud, whether we are talking about regulating relations between private parties (civil liability) or between individuals and states (for example, criminal investigation), or larger regional bodies such as the EU, or concerned with federated entities or special administrative regions such as Hong Kong. The chapter shows that zoning of the cloud
and Internet is emerging, if not already in operation, and that it is likely to speed up if cloud computing ever reaches its full potential.

Chapters 7 to 10 can be seen as forming the second part of this book, as each of their authors has chosen to elaborate upon various substantive areas of law in relation to cloud computing. In Chapter 7, Chris Reed points out that cloud users, and those whose information is processed by cloud providers, are naturally concerned that they may somehow lose their legal rights to that information once it enters the cloud. They are also concerned, or at least ought to be concerned, about who has the rights to the metadata and other information that cloud service providers generate in using that information. Reed argues that rights analysis is not the appropriate way to address this issue. Copyright law and the law of confidential information establish quite clearly who possesses these rights, and use of the cloud does not generally overturn them. What the cloud does instead is radically change the degree of control a rights owner has over the use and disclosure of information. To a certain extent, this is a matter that can be addressed in contracts, but building a contractual framework that incorporates all necessary cloud players is cumbersome and difficult. Most of the related issues can be more appropriately resolved through the establishment of cloud community norms, incorporated in appropriate governance mechanisms, and through greater accountability on the part of cloud actors concerning how information has and will be used.

Directly on the subject of copyright, Chapter 8 delves into questions about how the collection, handling and distribution of content and personal information can be appropriately undertaken in the new cloud environment. George Tian examines the recent development of cloud-related content regulations in various jurisdictions (the US, the UK, the EU, Japan, China and Australia) from a macro policy development perspective. A number of recent cases highlighting the potential for new and emerging cloud computing services to infringe copyrights or enable their customers to do so are discussed. Drawing lessons from the US and Australia, Tian provides practical suggestions for future content regulation and policy reform in Asia.

Revolving around the theme of copyright, Peter Yu in Chapter 9 explores how cloud platforms can be used to facilitate the worldwide distribution of copyrighted entertainment content. He examines the problems posed by existing markets, which are segmented based on legal and territorial boundaries and distribution and licensing arrangements. Yu then discusses how cloud platforms can better meet consumer demand for entertainment content in a highly globalized world. The chapter outlines the potential challenges and complications that arise from the
use of cloud platforms and distributors, and offers preliminary suggestions for the changes that are needed in the legal, business and technological environments.

Moving on from copyright concerns, Terry Kaan in Chapter 10 explores the challenges and concerns specific to the storage and use of healthcare information in the cloud. He sounds a note of caution in arguing that, in the rush to embrace cloud technology, insufficient attention has been paid to the much more fundamental issues and challenges raised by the transformation of data from analogue to digital form. In economically and technologically advanced countries, healthcare information is rapidly being moved from the analogue to the digital domain. Whilst it is widely assumed that the basic nature of the information remains essentially unchanged in this transformation, this chapter makes the argument that it in fact inevitably entails fundamental changes to the very nature of the stored information. By analyzing the experience of several jurisdictions, Kaan makes a general inquiry into the challenges and pitfalls that institutional data owners, policy planners and IT database system designers need to keep in mind when preparing to store healthcare information in the digital and cloud domains.

The remaining two chapters more pointedly underscore the practical concerns of cloud technology for researchers and for those parties involved in licence agreements. In Chapter 11, Edward Dove, Yann Joly and Bartha Knoppers remind us that the biggest challenge in 21st century data-intensive genomic science is developing the vast computer infrastructure and advanced software tools necessary to perform comprehensive analyses of genomic datasets for biomedical research and clinical practice. Researchers are increasingly turning to cloud computing both as a solution to integrate data from genomics, systems biology, and biomedical data mining and as an approach to analyzing data to solve biomedical problems. Whilst cloud computing provides several benefits, such as lower costs and greater efficiency, it also raises a number of legal issues. In this chapter, the authors discuss several key legal issues (data control, security, confidentiality, transfer and accountability) from an international legal perspective and based on a review of several publicly available cloud service providers’ terms of service. These issues should be borne in mind by genomic research organizations when they negotiate legal arrangements for storing genomic data on the servers of large commercial cloud service providers. Diligent genomic cloud computing means leveraging security standards and evaluation processes as a means to protect data, and entails many of the same good privacy practices that researchers should always consider in safeguarding local infrastructure.
In Chapter 12, Alan Chiu and Geoffrey Master revisit the issue of data ownership but from the perspective of content licensing. They ask this question: when a user uploads data to the cloud, whether in the form of a photo, text, soundtrack or logo, has he or she surrendered any ownership rights of that data? The answer depends very much on the nature and scope of the content licence agreed between the parties concerned. Content licences generally apply in any cloud computing context. The scope of that licence, defined in the terms of service agreement, often varies in accordance with the nature and features of the cloud services being used. There are typically significant differences between the licensing terms of public and private clouds. In this final chapter, the authors provide an overview of intellectual property (IP) licensing on the Internet, particularly in the context of cloud services, and discuss in detail some of the challenges to licensing in the cloud computing arena. They also discuss other intellectual property considerations that arise when engaging cloud services for private or business use. The chapter concludes with some thoughts about the future for IP licensing in cloud services.

Careful readers are likely to spot an inconsistency in this collection, that is, the use of ‘data’ as both a singular and a plural by different authors. As international consensus has yet to be reached over which usage is correct, the editors have decided to let the inconsistency remain. Our task is to provide useful navigational tools for crossing and recrossing the frontier between theory and practice, between regulation and innovation, and to clear away some of the clouds along the meandering path of law and technology.