Table of Contents

List of abbreviations 19

CHAPTER 1. Introduction 21
   a. Reasoning of the project and current state of affairs 21
      i. The European state of affairs 25
      ii. The US state of affairs 27
      iii. Current state of affairs in other countries 29
   b. Research question and structure of the project 30

CHAPTER 2. Cloud computing; a historical and technical overview 33
   a. Introduction – scope of this chapter 33
   b. A brief history of the cloud 34
   c. The NIST definition of cloud computing; a starting point 36
   d. The technologies that preceded cloud computing; a brief overview and comparison 39
      i. Cloud computing compared to traditional IT – Their main differences and why the cloud matters 39
      ii. Cloud computing environments compared to client-server systems 41
      iii. Cloud computing compared to outsourcing – The key differences 42
   e. Data handling needs and the parallel technological evolution – How developing computational requirements led to technological progress 44
   f. Explaining cloud computing and its predecessors – what did the cloud replace and what is now done different than before? 45
      i. File hosting 46
      ii. Clustering 46
      iii. Grid Computing 47
      iv. Virtualization 48
   g. Cloud computing: its core philosophy and structural features 48
      i. The cloud’s business model 49
ii. The architecture of cloud computing systems 49
h. The resource management aspects of the cloud 50
   i. The cloud’s compute model 50
   ii. Virtualization 51
   iii. Monitoring 52
   iv. Provenance 53
i. The application model of the cloud 53
j. The security model of the cloud 54
k. What is cloud computing after all and why does it merit a new regulatory approach? 56

CHAPTER 3. EU vs. US: the two major schools of thought regarding internet and privacy regulation and why they took divergent paths. Can this distance be bridged in the context of a regulatory framework for the cloud? 58

a. Introduction – scope of the chapter 58
b. How extensive is the influence of European data privacy standards outside Europe? Is it EU law that has been so influencing or is it more the entire European legal thinking? 59
c. What is the main difference from Europe in USA’s arrangement of their regulatory framework for privacy and the internet? 63
d. The ‘privacy collision’ between Europe and the USA: a brief historical overview 64
e. Personal data privacy in Europe and the US: a pragmatic and an articulate approach 70
f. Cyber challenges and state-of-the-art in Europe and the USA 73
   i. EU’s approach towards cyber challenges 73
   ii. The US approach towards cyber challenges 75
g. Can cloud computing be a tipping point for regulating and thinking about privacy in the US or Europe? 76
   i. Privacy under the effect of the cloud in the US 77
   ii. Judicial obstacles 78
   iii. Legislative obstacles 79
   iv. Societal obstacles 80
h. Europe’s combined approach towards the cloud and economic growth 81
i. A close look on how the EU and the US currently handle sensitive consumer data on the cloud. Is the current regime adequate and efficient enough?

   i. Regulating privacy and security of consumer sensitive data in the cloud; the US current status quo
   ii. Regulating privacy and security of consumer sensitive data in the cloud; the EU current status quo
   iii. The need for efficient protection of sensitive data also points towards regulatory reform in the cloud

CHAPTER 4. An introduction to the definition of cloud computing under EU law and the challenges it poses

   a. Introduction – scope of this chapter
   b. The most important policy views on aspects of cloud computing brought out so far and why they are not yet sufficient
   c. The European Data Protection Directive 95/46/EC; an assessment of its effects on the prevalent views about data protection and related IT technologies; are things different under the GDPR?
   d. Focus on the General Data Protection Regulation: is the European Union’s brand new law already insufficient to effectively regulate the cloud?
      i. Does the GDPR set up a truly universal legal framework for data transfer law?
      ii. What does the spirit of GDPR tell us about the longevity of the current overall EU data protection regime?
   e. GDPR and its readiness to respond to big scale uses of data in the cloud; the case of machine learning
   f. Vision for a cloud-based future
   g. The road from data privacy to cloud computing regulation
      i. Privacy and security viewed through the years and across major jurisdictions
      ii. Privacy issues particular to cloud computing technologies
      iii. Why does cloud computing call for a new regulatory framework?
CHAPTER 5. Legal pluralism and harmonization – how can we reach a common minimum understanding on how to regulate the cloud?

a. Introduction – scope of this chapter
b. Internet Regulation: a paramount of unilateralism
c. From governments to governance; learning to do laws for a borderless world
d. So far, existing laws about cyberspace are bad laws. Lessons learnt?
e. Lex informatica: The formulation of policy rules for the web through applied technology. Can it offer any useful insight for the conceptualization of a dedicated cloud computing regime?
f. Sectoral codes of conduct: the most dedicated attempt to come up with cloud computing laws so far and how it could be improved
g. Efforts undertaken so far on the front of sector-based regulation of IT and their common weakness
h. Seeking the way forward on cloud computing regulation in the field of global administrative law
   i. Defining global administrative law
   ii. The general theory on global administrative law and its principles
   iii. Theoretical foundations of global administrative law based on US and EU administrative law
i. Legal pluralism in global administrative law
   i. The proposal
   ii. The problems of legal pluralism
j. Can effective cloud computing regulation be achieved through international law? Not really.
k. A comparatist approach and synthesis is the only way; moving forward to regulate cloud computing through legal pluralism

CHAPTER 6. Jurisdiction and accountability in the cloud

a. Introduction – scope of this chapter

PART I: Jurisdiction in the era of cloud computing
a. The currently prevailing legal norms in EU law for claiming jurisdiction over cases involving data transfer and processing
   i. Establishment - Art. 4 para. 1(a) DPD
   ii. International law - Art. 4 para. 1(b) DPD
   iii. Equipment - Art. 4 para. 1(c) DPD
   iv. Changes to current status quo by the upcoming GDPR
b. Technology and internet jurisdiction: a process of parallel 'give and take'
c. From data protection law to international jurisdiction on the internet; adapting laws to modern needs and reality
d. What is the problem with asserting jurisdiction over cloud-related cases under current EU laws?
e. Steps to reduce jurisdictional disputes from the perspective of EU law
f. The internet jurisdiction risk of cloud computing under US law
   i. The basics about determining jurisdiction under US law
   ii. Jurisdiction under the influence of technological evolution; practices for alleviating jurisdiction risks in the US and internationally over IT-related cases
g. Corporate strategy as a pre-emptive measure for facing the long arm of cloud jurisdiction
   i. Virtual and physical environments
   ii. Accepting the inherent nature of cloud jurisdiction risk
h. Where are cloud data centers located? How jurisdiction plays a major part in deciding on geographic location, economic and environmental parameters in cloud computing

PART II: Accountability on the cloud
a. Accountability: the essentials from data protection to cloud computing
b. Accountability is not self-regulation; clearing the picture between two comparable but critically different concepts
c. Accountability in the cloud cannot be sufficiently settled with existing EU laws
d. Providing answers to the privacy challenges of cloud computing under US law; the importance of the Fourth Amendment principles
CHAPTER 7. Risks and compliance in cloud computing environments – views from Europe and the USA 202

a. Introduction – scope of this chapter 202

PART I: THE RISKS ASSOCIATED WITH CLOUD COMPUTING 202

a. Privacy issues raised on the cloud: existent for all kinds of data across all types of cloud networks 202
   i. United States v. Miller 205
   ii. The Electronic Communications Privacy Act (ECPA) – a step ahead but obscurity lingers 206
   iii. The USA PATRIOT Act 207
   iv. The HIPAA and compelled disclosures 207
   v. The Fair Credit Reporting Act 209
b. Threats to privacy means threats to security: the two prominent issues that go hand in hand in cloud computing environments 210
c. Privacy risks posed by the cloud put into question cornerstone elements of information privacy laws 213
d. The other side of the coin: how cloud computing’s architectural advantages can turn into threats for privacy 216
e. The affluence of consumer data on cloud computing and particular threats to them because of the cloud’s specificities 218
f. Reviewing security, privacy and trust issues on the cloud from an EU perspective 221

PART II: CLOUD COMPLIANCE 224
a. Introductory remarks on the concept of ‘cloud compliance’ 224
b. Effective regulation of technology: the need to define policy tools and policy actors 225
c. Incorporating users’ privacy concerns into the rules governing design and deployment of cloud environments 227
d. Pragmatic answers regarding the deployment of secure and privacy-proof cloud networks 231
e. Incentivizing privacy and security by encouraging the adoption of privacy enhancing technologies 232

CHAPTER 8. Principles for regulating the cloud (1); conclusions from the ontology of cloud computing networks 234

a. Introduction – scope of this chapter 234
b. Constructing the ontology of the cloud; is the cloud one and only thing after all? 235
   i. The Firmware/Hardware layer 238
   ii. The Software Kernel layer 238
   iii. The Cloud Software Infrastructure layer 240
   iv. The Cloud Software Environment layer 242
   v. The Cloud Application layer (SaaS) 242
c. Different uses but the same ontology: what does this mean for cloud computing regulatory principles? 243
d. Mapping the life cycle of data on cloud computing networks: risks, security and privacy issues as indicators for the nature of cloud computing regulation rules 245
   i. Data generation 246
   ii. Transfer 247
   iii. Use 247
   iv. Sharing 248
   v. Storage 249
   vi. Archival 251
   vii. Destruction 251
e. Regulatory principles derived from the ontology of cloud computing 252
   i. On the hardware/firmware layer 252
   ii. On the software/kernel layer 255
   iii. On the cloud software infrastructure layer 256
   iv. On the PaaS and SaaS layers 257
v. On the SaaS layer in particular

CHAPTER 9. Principles for regulating the cloud (2); based on the roles and functions across the cloud workflow

a. Introduction – scope of this chapter
b. Viewing cloud computing from the outside; what else is the cloud apart from its infrastructure and the science behind it?
c. Completing the picture of the inner side of the cloud; regulatory challenges stemming from the cloud network’s business workflow
   i. The customer (or user) of cloud computing services
   ii. The service provider
   iii. Infrastructure providers
   iv. Aggregate services providers (aggregators)
   v. The platform provider
   vi. The cloud services consultant
d. The innovative nature of cloud computing business and the legal challenges raised as a result thereof
e. Summarizing the issues raised by the new modus operandi established in IT market by cloud computing; where is there a need for new cloud computing rules and what precisely should their content be?
   i. Data protection
   ii. Data Security
   iii. Data retention
   iv. Consumer protection
   v. Intellectual Property
   vi. Competition
   vii. Trade
   viii. Jurisdiction, applicable law, enforcement
   ix. Compliance
   x. Transparency
   xi. Responsibility and liability
   xii. Infrastructure
f. What challenges lie ahead in designing cloud computing regulation rules?
   i. Challenges in conceptualizing cloud computing regulation
CHAPTER 10. Principles for regulating the cloud (3); the adoption of cloud computing regulation as the big leap forward from governing to governance in IT law

a. Introduction – scope of this chapter
b. Doing laws based on the local and global experience: the differences in approach and the need to combine both perspectives in the case of cloud computing
c. The ability of law to learn and evolve; how to achieve law evolution in the case of cloud computing
d. How proportionality and teleological reasoning can help cloud computing regulation make IT laws overall more efficient
e. How technology itself can help establishing a sound system of governance in the field of cloud computing
f. The key to achieving a sound system of governance in cloud computing regulation: legal interoperability and its significance as a concept in transnational law
g. A brief summary of the trends on privacy regulation through time in a global context; the transit to a cloud computing regulation governance regime is not a free fall into the unknown
h. Making a long-lasting governance regime a choice not a necessity
i. Can the transatlantic divide on privacy be bridged? Why the extensive use of cloud computing technologies makes the call for convergence an urgent one?

CHAPTER 11. Conclusion

a. The driving forces that make the need for cloud computing regulation a pressing one
b. Overview of solutions and suggestions towards the development of sound cloud computing regulation regimes
   i. Normative proposals
   ii. Governance proposals
iii. Policy proposals 347
   c. Future challenges – insights for further research 349

List of laws and statutes 353

List of case law 351

Bibliographical index 355