Schriften der Albrecht Mendelssohn Bartholdy Graduate School of Law

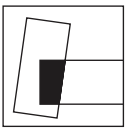
6

Xenofon Kontargyris

IT Laws in the Era of Cloud Computing

A Comparative Analysis between EU and US Law on the Case Study of Data Protection and Privacy

Nomos



Albrecht Mendelssohn Bartholdy
Graduate School of Law

Schriften der Albrecht Mendelssohn Bartholdy
Graduate School of Law

edited by

Prof. Dr. Stefan Oeter,
Lehrstuhl für Öffentliches Recht, Völkerrecht und ausländisches öffentliches Recht, Universität Hamburg

Prof. Dr. Tilman Repgen,
Lehrstuhl für Deutsche Rechtsgeschichte, Privatrechtsgeschichte der Neuzeit und Bürgerliches Recht, Universität Hamburg

Prof. Dr. Hans-Heinrich Trute,
Lehrstuhl für Öffentliches Recht, Medien- und Telekommunikationsrecht, Universität Hamburg

Band 6

Xenofon Kontargyris

IT Laws in the Era of Cloud Computing

A Comparative Analysis between EU and US Law on the Case Study of Data Protection and Privacy

Nomos

Gefördert durch einen Druckkostenzuschuss der Albrecht Mendelssohn Bartholdy Graduate School of Law.

Funded by a print subsidy from Albrecht Mendelssohn Bartholdy Graduate School of Law.

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

a.t.: Hamburg, Univ., Diss., 2018

Original title: "ICT LAWS IN THE ERA OF CLOUD COMPUTING – A comparative analysis between EU and US law on the case study of data protection and privacy"

ISBN 978-3-8487-5362-8 (Print)
978-3-8452-9562-6 (ePDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 978-3-8487-5362-8 (Print)
978-3-8452-9562-6 (ePDF)

Library of Congress Cataloging-in-Publication Data
Kontargyris, Xenofon
IT Laws in the Era of Cloud Computing
A Comparative Analysis between EU and US Law on the Case Study of Data Protection and Privacy
Xenofon Kontargyris (ed.)
378 p.
Includes bibliographic references and index.

ISBN 978-3-8487-5362-8 (Print)
978-3-8452-9562-6 (ePDF)

1st Edition 2018

To my parents, who have been my greatest supporters even at times that I did not believe so strongly in myself.

Στους γονείς μου, που πιστεύουν πάντα σε μένα ακόμα κι όταν ο ίδιος δεν πιστεύω τόσο δυνατά στον εαυτό μου.

To my brother, who made sure that over the past three years no emergency would distract me from my goal.

Στον αδερφό μου, που τα τρία αυτά χρόνια δεν επέτρεψε σε απρόοπτα να με αποσπάσουν από το στόχο μου.

Foreword

I do not consider myself a genius. Over the course of my studies I have had the good fortune to meet and collaborate with colleagues and teachers who have razor sharp minds for science; I certainly do not feel I am one of them. Therefore, I am not one of those researchers who had been confident that they would sit down and conduct a PhD since their first day at University. Nevertheless, I have been lucky enough to be inspired and encouraged in the course of my academic life by friends, colleagues and teachers who saw potential in me and made me believe that everything is possible with hard, systematic work. Through this note, I would like to express my heartfelt gratitude firstly to Prof. Trute for giving me the chance to undertake this particular project despite the interdisciplinary challenges it posed for a lawyer; to Prof. Schulz for being an excellent second supervisor helping me to maintain the dual approaches between law and IT and between EU and US law that the challenge I had set up for myself necessitated; to Prof. Papadopoulou from my alma mater, the Aristotle's University of Thessaloniki, for offering me as much help and support as possible in order to remain academically sharp while I was looking for a suitable opportunity to conduct a project as demanding as an interdisciplinary PhD; to my ex-colleagues at Apogee Information Systems, my first full-time employer and at the Directorate General for Media at the European Commission for facilitating my curiosity to get to know the real meaning of terms such as 'software', 'data processes', 'cloud-based systems' etc., which are always intriguing for an IT lawyer but require a lot more than a strong legal background in order to tackle regulatory challenges associated to them. And last but not least, I wish to cordially thank all those classmates and teachers from my school years and the colleagues, friends and teachers from my university years who helped me build the confidence it took to make it from high school to my LLB study, then on to my LLM and further onwards to my PhD term. Regardless of degrees and titles, all these people and experiences have taught me that everything is possible if you are determined to fight for it. And this is a lesson I will cherish for life!

This work has been finalized on 27 September 2017. All its contents and arguments should be read in light of the legal status quo applicable at that time.

PS: Grandma, I know you are happy about this. I promise you I will not stop here!

Hamburg, 27. September 2017

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. It the current regime adequate and efficient enough? 82
i. Regulating privacy and security of consumer sensitive data in the cloud; the US current status quo 84
ii. Regulating privacy and security of consumer sensitive data in the cloud; the EU current status quo 85
iii. The need for efficient protection of sensitive data also points towards regulatory reform in the cloud 86

CHAPTER 4. An introduction to the definition of cloud computing under EU law and the challenges it poses 89

a. Introduction – scope of this chapter 89
b. The most important policy views on aspects of cloud computing brought out so far and why they are not yet sufficient 92
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? 96
d. Focus on the General Data Protection Regulation: is the European Union's brand new law already insufficient to effectively regulate the cloud? 101
i. Does the GDPR set up a truly universal legal framework for data transfer law? 103
ii. What does the spirit of GDPR tell us about the longevity of the current overall EU data protection regime? 105
e. GDPR and its readiness to respond to big scale uses of data in the cloud; the case of machine learning 109
f. Vision for a cloud-based future 112
g. The road from data privacy to cloud computing regulation 113
i. Privacy and security viewed through the years and across major jurisdictions 113
ii. Privacy issues particular to cloud computing technologies 115
iii. Why does cloud computing call for a new regulatory framework? 116

CHAPTER 5. Legal pluralism and harmonization – how can we reach a common minimum understanding on how to regulate the cloud? 118

a. Introduction – scope of this chapter 118
b. Internet Regulation: a paramount of unilateralism 119
c. From governments to governance; learning to do laws for a borderless world 122
d. So far, existing laws about cyberspace are bad laws. Lessons learnt? 125
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? 129
f. Sectoral codes of conduct: the most dedicated attempt to come up with cloud computing laws so far and how it could be improved 131
g. Efforts undertaken so far on the front of sector-based regulation of IT and their common weakness 136
h. Seeking the way forward on cloud computing regulation in the field of global administrative law 138
    i. Defining global administrative law 138
    ii. The general theory on global administrative law and its principles 140
    iii. Theoretical foundations of global administrative law based on US and EU administrative law 141
i. Legal pluralism in global administrative law 143
    i. The proposal 143
    ii. The problems of legal pluralism 146
j. Can effective cloud computing regulation be achieved through international law? Not really. 148
k. A comparatist approach and synthesis is the only way; moving forward to regulate cloud computing through legal pluralism 151

CHAPTER 6. Jurisdiction and accountability in the cloud 153

a. Introduction – scope of this chapter 153

PART I: Jurisdiction in the era of cloud computing 153

a. The currently prevailing legal norms in EU law for claiming jurisdiction over cases involving data transfer and processing 153
i. Establishment – Art. 4 para. 1(a) DPD 154
ii. International law – Art. 4 para. 1(b) DPD 157
iii. Equipment – Art. 4 para. 1(c) DPD 158
iv. Changes to current status quo by the upcoming GDPR 158
b. Technology and internet jurisdiction: a process of parallel 'give and take' 161
c. From data protection law to international jurisdiction on the internet; adapting laws to modern needs and reality 164
d. What is the problem with asserting jurisdiction over cloud-related cases under current EU laws? 168
e. Steps to reduce jurisdictional disputes from the perspective of EU law 170
f. The internet jurisdiction risk of cloud computing under US law 173
i. The basics about determining jurisdiction under US law 173
ii. Jurisdiction under the influence of technological evolution; practices for alleviating jurisdiction risks in the US and internationally over IT-related cases 176
g. Corporate strategy as a pre-emptive measure for facing the long arm of cloud jurisdiction 178
i. Virtual and physical environments 178
ii. Accepting the inherent nature of cloud jurisdiction risk 179
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 179

PART II: Accountability on the cloud 181

a. Accountability: the essentials from data protection to cloud computing 181
b. Accountability is not self-regulation; clearing the picture between two comparable but critically different concepts 183
c. Accountability in the cloud cannot be sufficiently settled with existing EU laws 185
d. Providing answers to the privacy challenges of cloud computing under US law; the importance of the Fourth Amendment principles 187

e. Achieving effective regulation of the cyberspace: discussing particularities of the web and how these should be mirrored in modern laws about aspects of the digital world 190
f. Tackling the issue of perspective in internet law; an essential step towards a pragmatic accountability regime 193
g. The road to an accountable cloud computing goes through the road to an accountable internet: how to achieve a sound internet governance 196
h. Effective accountability for cloud computing 197
i. Accountability as a way to further reinforce privacy in the cloud 199

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 258

CHAPTER 9. Principles for regulating the cloud (2); based on the roles and functions across the cloud workflow 261

a. Introduction – scope of this chapter 261
b. Viewing cloud computing from the outside; what else is the cloud apart from its infrastructure and the science behind it? 262
c. Completing the picture of the inner side of the cloud; regulatory challenges stemming from the cloud network's business workflow 267
i. The customer (or user) of cloud computing services 270
ii. The service provider 272
iii. Infrastructure providers 275
iv. Aggregate services providers (aggregators) 277
v. The platform provider 278
vi. The cloud services consultant 278
d. The innovative nature of cloud computing business and the legal challenges raised as a result thereof 279
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? 282
i. Data protection 282
ii. Data Security 283
iii. Data retention 284
iv. Consumer protection 285
v. Intellectual Property 286
vi. Competition 286
vii. Trade 287
viii. Jurisdiction, applicable law, enforcement 288
ix. Compliance 289
x. Transparency 289
xi. Responsibility and liability 290
xii. Infrastructure 290
f. What challenges lie ahead in designing cloud computing regulation rules? 291
i. Challenges in conceptualizing cloud computing regulation 291

ii. Challenges in implementing cloud computing regulation 294
iii. Projecting challenges in the assessment phase of a regulation on the cloud 297

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 301

a. Introduction – scope of this chapter 301
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 301
c. The ability of law to learn and evolve; how to achieve law evolution in the case of cloud computing 309
d. How proportionality and teleological reasoning can help cloud computing regulation make IT laws overall more efficient 313
e. How technology itself can help establishing a sound system of governance in the field of cloud computing 316
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 321
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 325
h. Making a long-lasting governance regime a choice not a necessity 327
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? 329

CHAPTER 11. Conclusion 335

a. The driving forces that make the need for cloud computing regulation a pressing one 335
b. Overview of solutions and suggestions towards the development of sound cloud computing regulation regimes 338
i. Normative proposals 338
ii. Governance proposals 345

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

List of abbreviations

(in alphabetical order)

Amazon Web Services	AWS
Application Programming Interface	API
Application Service Provision	ASP
Artificial Intelligence	AI
Asian-Pacific Economic Cooperation	APEC
Binding Corporate Rules	BCR
Charter of Fundamental Rights of the European Union	CFREU
Chief Executive Officer	CEO
Cloud Service Provider	CSP
Communication as a Service	CaaS
Communications Decency Act	CDA
Community Based Participatory Research	CBPR
Customer Relationship Management	CRM
Data as a Service	DaaS
Data Protection Directive (European)	DPD
Digital Millennium Copyright Act	DMCA
Electronic Communications Privacy Act	ECPA
European Convention on Human Rights	ECHR
European Economic Area	EEA
European Union	EU
Fair Credit Reporting Act	FCRA
Federal Trade Commission (US)	FTC
Foreign Intelligence and Surveillance Act	FISA
General Data Protection Regulation (European)	GDPR
Hardware as a Service	HaaS
Health Insurance Portability and Accountability Act	HIPAA
Information & Communications Technology	ICT
Information Technology	IT
Infrastructure as a Service	IaaS

Internet Corporation for Assigned Names and Numbers	ICANN
Internet of Things	IoT
Internet Service Provider(s)	ISP(s)
Local Area Network	LAN
National Institute of Standards and Technology	NIST
Official Journal (of the European Union)	OJ
Operating System	OS
Organization for Economic Co-operation and Development	OECD
Platform as a Service	PaaS
Platform for Privacy Preferences Project	P3P
Privacy Enhancing Technologies	PETs
Remote Computing Service	RCS
Secure Sockets Layer	SSL
Service Oriented Architecture	SOA
Service as a Service	SaaS
Software as a Service	SaaS
Stored Communications Act	SCA
Terms of Service (agreement)	ToS (agreement)
Transport Layer Security	TLS
Treaty on the European Union	TEU
United Nations Commission on International Trade Law	UNCITRAL
United Nations Universal Declaration of Human Rights	UDHR
United States (of America)	US(A)
United States of America: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act	USA PATRIOT Act
Virtual Machine(s)	VM(s)

CHAPTER 1. Introduction

a. Reasoning of the project and current state of affairs

Since the cloud has started gaining popularity, one of the catch-phrases used about it by supporters and adversaries alike and which can indeed be read in a positive or negative manner, depending on one's predisposition, has been: "There is no cloud. It's just someone else's computer."[1] Cloud computing made its entry in the IT industry as a revolution which was meant to profoundly alter the way most of IT and digital data business had been done till then[2]. Indeed, despite the partial loss of control over data that comes immediately with its use, cloud computing has been massively successful and, apart from average users' data, a great variety of critical records are also being entrusted to it, generating ever-growing concerns about their integrity, privacy and security.

In the face of these trends around the cloud and its uses, privacy and security have grown into two somewhat competing forces attempting to balance opposing needs: privacy focuses on the need to use information against the need to protect personal data, while security is centered on the need to provide access to records against the need to stop unauthorized access[3]. The importance of these competing goals has led to a plethora of legal and regulatory ventures to strike a balance and, ultimately, to achieve a certain level of trust in digital records and their storage in the cloud[4]. A particular challenge to the whole effort has come to be the fact that different jurisdictions approach privacy in substantially different manners while an in-depth understanding of what a jurisdiction's laws may aim at, or under the rules of what particular jurisdiction certain data may be governed,

---

1 Tom Geller, *In privacy law, it's the U.S. vs. the world*, 59 Commun. ACM 21–23 (2016.)

2 See also Chapter 2.

3 Luciana Duranti, Trust in online records and data. Integrity in Government through Records Management: Essays in Honour of Anne Thurston.

4 D. Hofman, Duranti L. & E. How, *Trust in the Balance*. *Data Protection Laws as Tools for Privacy and Security in the Cloud*, 10 Algorithms 47 (2017.)

requires a tremendous analytical effort. Nonetheless, in order to protect privacy and enhance security, this effort is unavoidable.

Should one look for a single phrase to summarize why cloud computing does make a difference in the way we are handling digital information and why we should regulate all this information processing having cloud computing in our focus, a suitable passage could be the following: …"preserving information in the cloud may be a black box process in which we know, at least ideally, what we put in for preservation, and we know what we want to access and retrieve—essentially the same things we put in—but often we do not know what technology is used by cloud service providers to manage, store, or process our information"[5].

Even in the ideal case in which there was no intended malice by actors involved in the cloud, data record keeping and processing done via cloud computing poses a number of unanswered questions. As Duranti and Rogers have most recently categorized them[6], those challenges broadly refer to: managing trans-jurisdictional data flows, attributing liability for and resolving data breaches, and establishing the chain of custody when a cloud service provider goes dark[7]. Given these risks, one might wonder why people continue to trust the cloud so strongly and at such a growing pace. The answer, as it will be demonstrated soon[8], is that, from a technological efficiency point of view, there is no better option in the realm of the internet-driven world right now and the cloud stands out by far from all other available technologies. Of course, the greatest ally in dealing with such risks is constant technological innovation itself, which tries hard to keep pace with malicious and innocent challenges of the cloud alike and ensure the trustworthiness of records stored on it. However, approaches based solely on technical means cannot solve the problems that arise from technology and its maluses; besides, there is no technical solution to determined human misuse of technology, to say the least[9]. In fact, technological tools need support from legal, social, and business structures that set the

5 Luciana Duranti, Adam Jansen, Giovanni Michetti, Mumma Courtney, Daryll Prescott, Corinne Rogers & Thibodeau Kenneth, *Preservation as a Service for Trust*, in Security in the private cloud, 47–72 (John R. Vacca ed., 2017.)

6 *Id.*

7 This issue does not form part of this analysis which solely focuses on the public law aspects of cloud computing regulation, leaving civil or criminal law issues aside for future research.

8 See Chapter 2.

9 Luciana Duranti (note 3).

bar for minimum expectations from cloud service providers. While some users (particularly those heavily based on data storage and processing from their core operation model already) might indeed thoroughly analyze the "reputation, performance, competence, and confidence"[10] of cloud service providers to verify their trustworthiness and robustness, experience and market data show that the majority continue to be quite instinctive with the choice of whom they entrust with their data[11]. It is precisely for those cases – which probably constitute the majority anyway – where consumers rely upon a service without having sought assurances of its quality beforehand that the law must step in to provide the certainty and trust users cannot or did not bother to obtain on their own[12]. The typological diversity of records kept in cloud environments is forcing the law to modernize existing regulatory tools and improvise on new ones. Combined together, these tools aim to strike the balance described earlier: between long-standing concerns, namely access, control, security, and trust and a world where data have got considerably detached from the physical bonds that traditionally kept them within the borders of a single jurisdiction and the control of an identified and trusted custodian.

Discussing "privacy" as a legal pursuit is challenging to say the least; according to Solove, "Privacy seems to be about everything, and therefore it appears to be nothing"[13]. The very conception of privacy is widely contextual; as it has been argued, "our conceptions of privacy result from our juridified intuitions—intuitions that reflect our knowledge of, and commitment to, the basic legal values of our culture"[14].

On a broader basis, Americans' use of the term 'privacy' typically refers to "privacy as an aspect of liberty, the right to freedom from intrusions by the state"[15]. Consequently, American privacy laws tend to focus on the freedom to determine who and to what extent has access to one's

---

10 Luciana Duranti & Corinne Rogers, *Trust in digital records*. *An increasingly cloudy legal area*, 28 Computer Law & Security Review 522–531 (2012.)

11 Frank B. Cross, *Law and trust*, 93 The Georgetown Law Journal 1457–1545 (2005.)

12 Huaiqing Wang, Matthew K. O. Lee & Chen Wang, *Consumer privacy concerns about Internet marketing*, 41 Commun. ACM 63–70 (1998.)

13 Daniel J. Solove, *A Taxonomy of Privacy*, 154 University of Pennsylvania law review 477–560 (2006.)

14 James Q. Whitman, *The Two Western Cultures of Privacy*. *Dignity versus Liberty*, 113 The Yale Law Journal 1151–1221 (2004.)

15 For further analysis, see Chapter 3.

private life, particularly to the category of private information generally quoted as "personally identifiable information"[16]. From that perspective, gravity primarily lies with the possibility for a data subject to consent to their loss of privacy, while in laws developed under this prism the need for privacy is often juxtaposed by the need to use personally identifiable information for data subjects for countless different purposes. In contrast, the European concept of privacy views the term "as an aspect of dignity"[17]. The "juridified intuitions" on the foundations of European understandings of privacy cannot bear human dignity as a commodity. As a result, the American concept of 'privacy' coincides much better with the European notion of 'data protection'[18]. Both these policy areas on the two sides of the Atlantic seek to draw boundaries around information and records, putting up effective protection mechanisms for them from public or unauthorized private scrutiny. Such laws set off from the predicament that not all people can be trusted with all information[19]. In the pre-internet, offline era, this was operatively translated in controlling access to and, if necessary, retracting paper records containing sensitive information. However, under the profound impact of information and communications technologies on data and record keeping, along with an intensifying blur between "data" and "records," personally identifiable information can today be regarded as just a small subset of data[20], about which it cannot be said with certainty whether it is the original record or just an archived copy. However, this is a precarious approach as it strips the data off its context; an immediate effect is, for example, that we are no longer able to determine whether the data is 'private' for a particular purpose. Instead, by moving the protection focus at record, rather than data level, we could achieve better results. What is more, data mining and other big data techniques are increasingly rendering data-level privacy protection ineffective[21].

---

16 Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 New York University Law Review 1814–1894 (2011.)

17 James Q. Whitman (note 14).

18 *Id.*

19 Luciana Duranti (note 3).

20 Paul M. Schwartz & Daniel J. Solove (note 16).

21 Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Chris Hanson, James Hendler, Lalana Kagal, Deborah L. McGuinness, Gerald Jay Sussman & K. Krasnow

Based on these two poles, i.e. the European versus the American legal thinking about data protection and privacy, this study aims to take the decisive step and look into the matter from the broader perspective of technologies facilitating data processing and archiving of all kinds instead of the acts of processing and archiving per se. Those technologies are beyond doubt those collectively termed as 'cloud computing'. And because of the fact that legal research which aims to build up on an existing regime and provide better answers to tangible problems, which have nevertheless been around for a long time (with several laws that have already tried to tackle them thus making any new approach conditional to cohesion and not just innovative spirit), cannot set off from nowhere but needs to have one firm foot on actual acquis before it can take the leap forward, the starting point of endeavors of this study will largely, though not exhaustively, be privacy and data protection laws from Europe and the US.

i. The European state of affairs

The latest development out of deployment of cloud computing technologies, i.e. big data decision-making algorithms, are by nature meant to discriminate, to make distinctions based on voluminous data of a wide variety. An immediate challenge of algorithmic discrimination is the loss of judgment[22]. "The machine is incapable of determining whether a distinction is ethical or not. Unless we come up with a comprehensive theory of discrimination that can be represented algorithmically, we have no rigorous way of distinguishing between ethical and non-ethical machine-based discrimination [... however,] some of our ethical and moral criteria are so fragile, nuanced, and culturally dependent that it is not clear that the machine will ever be capable of appropriately weighing them"[23]. Still the data-driven approach to regulation of personally identifiable information runs on the assumption that by redacting or pseudonymizing the most sensitive kinds or parts of data set, we can prevent the algorithm from filling in missing information using the vast amounts of other data, quite possibly

---

Waterman, Transparent Accountable Data Mining: New Strategies for Privacy Protection (2006.)

22 Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. on Telecomm. & High Tech. L. 351–368 (2013.)

23 *Id.*

even from the same data subject, that has at its disposal. However, sealing certain bits of data which have been labeled as personally identifiable information while leaving all other data available and open to whatever techniques resourceful data holders can devise, is a lost battle. The current data-centric approach to privacy will be less and less effective in building up or maintaining trust in cloud-based records[24].

The brand new European General Data Protection Regulation (GDPR)[25] explicitly recognizes these challenges, and seeks to establish a higher standard of trust and security for EU citizens[26]. And while it does not categorically solve all big data challenges to privacy, it does provide a much firmer ground for European citizens to expect that their privacy will not be breached by resourceful data processors. Furthermore, the European Union provides a second line of legal protection for its citizens, as the GDPR directly cites Article 8(1) of the Charter of Fundamental Rights of the European Union (CFREU)[27] which has already been repeatedly interpreted as providing robust protection for the online version of the right to privacy[28]. However, the GDPR largely remains a technology agnostic

24 Jiahong Chen, *How the best-laid plans go awry. The (unsolved) issues of applicable law in the General Data Protection Regulation*, 6 International Data Privacy Law 310–323 (2017.)

25 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (OJ) L119, 4/5/2016, p. 1–88.

26 Recital 26 of the GDPR explicitly notes that, even though personal data may have undergone pseudonymization, "account should be taken of all of the means reasonably likely to be used […] to identify the natural person directly or indirectly," distinguishing between pseudonymized data and anonymous data.

27 Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

28 Recital 73 of the GDPR reads: "Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regula-

legislation[29], one that follows on the long path of data-focused EU privacy legislation, which is developed having specific existing or foreseeable applications of data-related technologies in sight instead of the specifications, present and foreseeable ones, of those technologies.

ii. The US state of affairs

The regulatory plateau in the US regarding phenomena occurring in the cloud, most prominently regarding the issue of how to gain access to data hosted on cloud environments, is substantially different to the one in Europe; not so much as to the aims it pursues or the genre of protection it wishes to grant to data subjects but rather on the way it has developed over the years and how it looks today[30]. Owing to the endemic differences of legal tools between Europe and America, in the US there is no central legislation regarding cloud data but rather several legal resources (from provisions of the US constitution, to Acts, to case law) which provide legal basis for regulating cloud-related phenomena. The global clouds on which the greatest part of the IT world operates today pose challenging questions regarding the scope of traditional legal tools governing these phenomena and, most importantly, the issue of access to data stored in cloud facilities outside the United States. The far from settled landscape on the issue can be observed even through latest case law with regard to the Stored Communications Act (SCA)[31]. Different decisions expose numerous unan-

---

ted professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behavior under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.".

29 For more extensive analysis on the GDPR and its shortcomings as well as the innovations it introduces refer to Chapter 4.

30 For a comparative analysis on the development of data protection and privacy law in Europe and the US refer to Chapter 3.

31 The Stored Communications Act (SCA), 18 U.S.C. Chapter 121 §§ 2701–2712. For more refer to Chapter 3.

swered questions about the conditions under which parties can obtain cloud data. Specifically, in litigation involving extra-territorial data requests under the SCA US courts have at times focused on where the requested data is located, and on other instances on where the search or seizure of it will take place[32]. In addition to the SCA, there are further statutory authorities that grant government and private parties the permission to make extra-territorial data requests, creating additional unresolved issues as well. What is more, American academia is also far from settled about the meaning of territoriality for data access[33]. This scattered playing field produces equally varying legal outcomes which themselves demonstrate how disconcerted existing US laws applying to the cloud are, their most alarming effect being that they powerfully incentivize international data localization[34]. Mandatory data localization is already a legal requirement in a number of countries such as Brazil and Russia, while there is additionally another important trend of voluntary data localization[35]. Both of them are, to a significant degree, fueled by concerns about US rules for data access, which make more and more non-US companies to choose to bind themselves to national or regional protections which recognize or demand data localization for cloud networks. However, in the long run, this trend risks seriously disrupting the Internet and undermining one of its fundamental characteristics, the lack of boundaries in the circulation of da-

---

32 For an overview of the latest trends and developments in US law and jurisprudence regarding data and access to them, especially in relation to the cloud and information hosted on facilities abroad, refer to: Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 Yale Law Journal 326–398 (2015); Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stanford Law Review 729–789 (2016); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 Stanford Law Review 285–329 (2014); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 University of Pennsylvania law review 373–419 (2014); David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*. *iCourts Working Paper Series, No. 33, 2015* International Journal of Constitutional Law (2015); Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313–388 (2013.)

33 Paul M. Schwartz, Legal Access to Cloud Information. Data Shards, Data Localization, and Data Trusts.

34 For a thorough analysis on the issue of mandatory and voluntary data localization, refer to: Anupam Chander & Uyen P. Le, *Breaking the Web*. *Data Localization vs. the Global Internet* Emory Law Journal, Forthcoming 53 (2014.)

35 *Id.*

ta and overall traffic[36]. Therefore, it is high time for the US to work with other jurisdictions, primarily with the EU, towards developing internationally harmonized rules for access to cloud information.

iii. Current state of affairs in other countries

In response to growing concerns about security and privacy of data in the cloud, regulators in jurisdictions around the world are turning to data localization measures[37]. These regulatory tools include laws, regulations, and policies designed to make sure that data and records are accessed, processed, and stored within a specific jurisdiction[38]. Data localization measures are conceptualized with the aim of fortifying the privacy rights of data owners whose records cross jurisdictional borders[39].

Briefly, data localization laws are based on the assumption that, if the jurisdictions in which records and data can be accessed, processed, and stored are limited, those records will be sealed against bad actors for whom laws from other jurisdictions would provide no effective recourse. Realistically speaking though, this is a problematic assumption[40]. Any records and data made available at some point online can eventually be accessed and harmed by malicious actors in almost any jurisdiction. And, of course, whether or not the jurisdiction in which the records are located can provide effect remedy in such an instance depends on more than just localization laws. Secondly, data localization laws assume that records hosted locally are by default more secure[41]. However, there is no guarantee for that; everything depends on adequate technical solutions and expertise being available within the jurisdiction where cloud services are provided. To put it plainly, it should not be taken for granted that there are actual data centers and hardware facilities by all cloud providers within the area of every single jurisdiction. In addition, data localization laws assume that local custody is a preferable means of protecting records and data and as-

---

36 Paul M. Schwartz (note 33).
37 Anupam Chander & Uyen P. Le (note 34).
38 *Id.*
39 *Id.*
40 Paul M. Schwartz (note 33).
41 Y. Tian, *Current Issues of Cross-Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement. Join or Withdraw*, 34 Wisconsin International Law Journal 367–408 (2016.)

suring their trustworthiness. However, this predicament invalidates the very important element of evaluation of trustworthiness that any cloud service provider, regardless of their size, should undergo in order to survive on the market according to internationally accepted market practice[42]. The last assumption is that data localization laws provide augmented stability should cloud services prove untrustworthy or insecure, because, at least, they provide clarity as to which jurisdiction's laws will apply in resolving the disputes that may arise. In reality, however, there is no better safeguard for security of records and data in the cloud than the trust mechanisms of the international cloud market, only by taking part in which can a cloud service provider, regardless of size, survive and remain competitive; thus, all CSPs will do whatever it takes to make sure they remain part of it[43].

b. Research question and structure of the project

Given the state of affairs described above, this project is going to look for ways for achieving better coordinated regulation of the cloud and the issues arising from using it. The stated aim will not be pursued though having in mind the establishment of an international regulatory framework for the cloud, let alone the introduction of some other type of supranational jurisdiction for cloud and IT-related phenomena. Instead, in an attempt to be realistic in the way the research question is approached in conjunction with the regulatory state-of-the-art across jurisdictions, the project's focus will be on pinpointing and bringing together best practices regardless of their origin which, if combined and taken into consideration as the foundations for the future development of cloud regulation laws by law makers from all legal orders will lead to a more coherent governance scheme for cloud computing. Logically, some of the suggestions put forward in the course of this analysis may not sound as ground-breaking for all readers, depending on whether each one of them is more familiar with the European or US legal thinking on the matter. However, the originality of this analysis lies precisely on drawing for the first time the best each and every school of thought has to offer under the same roof.

---

42 Nicholas Platten, *Protectors of Privacy: Regulating Data in the Global Economy – By A.L. Newman*, 48 JCMS: Journal of Common Market Studies 453–454 (2010.)

43 *Id.*

The forthcoming analysis should be read in light of the following understandings:

– Although from a technical point of view it is always easier to discern between cloud computing per se and specific applications made possible thanks to the cloud, this distinction has not yet been unquestioningly achieved on the regulatory front. Therefore, while the technical parts of this research invariably refer to cloud computing generically, in the parts of legal analysis it is mandatory to begin discourse from the laws currently applicable in order to understand how the current status has been consolidated and how steps forward could be taken. Therefore, in parts of this project where the legal dimension of the research question is dealt with the starting point is mostly, but not exclusively, existing laws about privacy, data protection and data transfers on the cloud. It is hoped that by applying the findings and suggestions presented throughout this study, current laws will move forward towards a more generic and less case-based direction, grasping the cloud phenomenon per se and not limiting their understanding to specific cloud applications.
– With regard to the jurisdictions and the origins of scholarly opinion that form part of this comparative analysis, it needs to be pointed out right from the beginning that there is a similar distinction between resources and literature of a technical and those of a legal nature. in particular, given that, from a technological perspective, the cloud is viewed in the same manner worldwide, this study utilizes relevant resources from a variety of origins (e.g. from European, American, Chinese and Canadian academics, to name a few). However, due to the greatly varied ways in which the cloud has been viewed so far from a legal point of view, only the laws and regulations of the EU and the US form part of this study. The two jurisdictions together account for the biggest part of the ways in which law makers currently deal with the cloud[44]. Moreover, this choice was also made due to practical factors, namely ease of access to resources, linguistic capabilities of the researcher (these two are the main reasons why the Chinese jurisdiction is left out of the scope of the project altogether) as well as time constraints for the completion of the project.

---

44 For more on the significance EU and US laws and markets play with regard to cloud computing refer to Chapter 3.

With the above understandings in mind, the chapters of the analysis that follow deal with these groups of challenges[45] regarding the prospect of a more consolidated regime on cloud computing regulation:

– The jurisdictional challenge, mainly dealt with in Chapter 6;
– The privacy and security challenge, mainly dealt with in Chapter 7;
– The convergence challenge, mainly dealt with in Chapters 8, 9 and 10.

45 Y. Tian (note 41).

CHAPTER 2. Cloud computing; a historical and technical overview

a. Introduction – scope of this chapter

Cloud computing technologies have been rapidly expanding over the past ten to fifteen years to be today the standard enabling technology for most of the applications and aspects of the internet as we know it. Cloud-based systems and cloud computing, as such, were not an invention, nor a pioneering discovery when they started to be widely commercialized in the beginning of 2000s. They had actually been around long before, as technically feasible arrangements for the handling of data and the execution of computational tasks. However, the growing appetite for processing power that an increasing e-economy necessitated, the commoditization of more and more internet-based services related to data handling and the equally fast rate at which consumers adopted these services led to a rapid commercialization of cloud technologies[46]. Yet, despite the fact that the cloud, as a technical feasibility, had been around since long before, its true meaning and the ways in which it did things differently than before had not been adequately realized or examined for many years after its popularization as a commodity. In order to understand what cloud computing is all about and, eventually, demonstrate what it does differently in comparison to previous technical arrangements for data handling tasks, a review of the history of the cloud is the first step.

Getting familiar with the essence of the technical aspects of cloud computing is the aim of this chapter of the study.

---

46 For more information on the history and technical evolution of cloud computing refer to: M. Arif, A history of cloud computing, available at: http://www.computerweekly.com/feature/A-history-of-cloud-computing (18 February 2015); Hongji Yang & Xiaodong Liu, Software reuse in the emerging cloud computing era (2012); Thomas Erl, Richardo Puttini & Zaigham Mahmood, Cloud computing. Concepts, technology, & architecture (2013); Antonio Regalado, Who Coined 'Cloud Computing'?, available at: https://www.technologyreview.com/s/425970/who-coined-cloud-computing/ (11 January 2017); Inc. Gartner, Cloud Computing Confusion Leads to Opportunity (2008).

b. A brief history of the cloud

Cloud computing has evolved to be the technology that we so extensively use today through a number of phases that included concepts like client-server arrangements[47], grid[48] and utility computing[49], application service provision (ASP)[50] and, more recently, Software as a Service (SaaS)[51].

On a visionary level, the idea of an "intergalactic computer network"[52] was for the first time formulated in the 1960s by Joseph Carl Rob-

47 The client–server model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. At most times, clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. (https://www.techopedia.com/definition/18321/client-server-model; last accessed on 01/11/2017.)

48 Grid computing is a collection of computer resources from multiple locations that are dedicated to reaching a common goal. The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files. (https://www.techopedia.com/definition/87/grid-computing; last accessed on 01/11/2017.)

49 Utility computing is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate. (https://www.techopedia.com/definition/14622/utility-computing; last accessed on 01/11/2017.)

50 Application Service Provisioning (ASP) is the business of providing computer-based services to customers over a network, such as access to a particular software application using a standard protocol (such as HTTP). (https://www.techopedia.com/definition/2476/application-service-provider-asp; last accessed on 01/11/2017.)

51 Software as a service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. (https://www.techopedia.com/definition/155/software-as-a-service-saas; last accessed on 01/11/2017.)

52 Intergalactic Computer Network or Galactic Network was a computer networking concept similar to today's Internet. The term was used for the first time in the early 1960s to refer to a networking system as an electronic commons open to all, ‘the main and essential medium of informational interaction for governments, institutions, corporations, and individuals.’ (https://en.wikipedia.org/wiki/Intergalactic_Computer_Network; last accessed on 01/11/2017.)

nett Licklider[53], who was responsible for facilitating the development of ARPANET[54] in 1969.

Licklider's vision was for everyone to be interconnected and able to access programs and data hosted at any site, from anywhere. "It is a vision that sounds a lot like what we are calling cloud computing"[55].

Another popular view is that the cloud concept was first envisaged by computer scientist John McCarthy who proposed the idea of computation being delivered as a public utility[56].

From a technical point of view, several decades went by with the know-how related to today's cloud-based systems already existing. Literally, cloud technologies were no invention and did not come as a result of a ground-breaking discovery. They were simply the outcome of better or, at least, different exploitation of existing knowledge related to IT systems[57]. One of the first milestones in cloud computing history was the arrival of

---

53 Joseph Carl Robnett Licklider was an American psychologist and computer scientist who is considered one of the most important figures in computer science and general computing history. He is particularly remembered for being one of the first to foresee modern-style interactive computing and its application to all kinds of activities; and also as an Internet pioneer with an early vision of a worldwide computer network long before it was built. (https://en.wikipedia.org/wiki/J._C._R._Licklider; last accessed on 01/11/2017.)

54 The Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet. ARPANET was initially funded by the Advanced Research Projects Agency (ARPA, later Defense Advanced Research Projects Agency, DARPA) of the United States Department of Defense. (https://www.techopedia.com/definition/2381/advanced-research-projects-agency-network-arpanet; last accessed on 01/11/2017.)

55 J. Locke, The Roots of Cloud Computing, available at: http://www.servercloudcanada.com/2013/10/the-roots-of-cloud-computing/ (11 January 2017); last accessed on 01/11/2017.

56 John McCarthy was an American computer scientist and cognitive scientist. McCarthy was one of the founders of the discipline of artificial intelligence. He coined the term "artificial intelligence" (AI), developed the Lisp programming language family, significantly influenced the design of the ALGOL programming language, popularized timesharing, and was very influential in the early development of AI. (https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist); last accessed on 01/11/2017.)

57 M. Arif (note 46).

Salesforce.com[58] in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The services firm paved the way for both specialist and mainstream software firms to deliver applications over the internet.

The next important step was Amazon Web Services[59] in 2002, which provided a suite of cloud based services including storage, computation and even human intelligence.

Another big milestone came in 2009, with the advent of Web 2.0[60], when Google and others started to offer browser-based enterprise applications through services such as Google Apps[61].

c. The NIST definition of cloud computing; a starting point

It has been so far impossible among stakeholders, namely, regulators, the IT industry etc., to agree on a universally acceptable definition of cloud computing. However, for the purposes of this study when reference is made to 'cloud computing' this is to be understood under the definition published in 2011 by the US National Institute of Standards and Technology (NIST); so far, this definition is generally heralded as the most preva-

---

58 Salesforce.com is a cloud computing company headquartered in San Francisco, California. Though its profits come basically from a customer relationship management (CRM) product, Salesforce also tries capitalizing on commercial applications of social networking through acquisition. (https://en.wikipedia.org/wiki/Salesforce.com; last accessed on 01/11/2017.)

59 Amazon Web Services (AWS) is a collection of remote computing services, also called web services, that make up a cloud computing platform offered by Amazon.com. These services are based in 11 geographical regions across the world. The most central and well-known of these services are Amazon Elastic Compute Cloud and Amazon S3. These products are marketed as a service to provide large computing capacity more quickly and cheaper than a client company building an actual physical server farm. (https://en.wikipedia.org/wiki/Amazon_Web_Services; last accessed on 01/11/2017.)

60 Web 2.0 describes World Wide Web sites that emphasize user-generated content, usability, and interoperability. Although Web 2.0 suggests a new version of the World Wide Web, it does not refer to an update to any technical specification, but rather to cumulative changes in the way Web pages are made and used. (https://en.wikipedia.org/wiki/Web_2.0; last accessed on 01/11/2017.)

61 Google Apps is a suite of cloud computing productivity and collaboration software tools and software offered by Google. (https://en.wikipedia.org/wiki/Google_Apps_for_Work; last accessed on 01/11/2017.)

lent[62] in explaining the 'cloud' and it reads as follows: "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. This cloud model is composed of five essential characteristics, three service models, and four deployment models"[63].

The most essential characteristics of cloud computing technologies and of the services developed based on them are[64]:

- **On-demand self-service**: A consumer can unilaterally calculate and preorder or buy in real time computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction with a salesperson or service provider;
- **Broad network access**: Services are available over the network and accessed through standard mechanisms that promote use by heterogeneous client platforms (e.g., mobile phones, tablets, laptops, and workstations);
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is an impression of location independence owing to the fact that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory and network bandwidth;
- **Rapid elasticity**: Resources can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward in accordance with demand. To the consumer, the resources available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time;

---

62 Bill Williams, The economics of cloud computing (2012.)

63 Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (4 November 2015.)

64 Thomas Erl, Richardo Puttini & Zaigham Mahmood (note 46).; Peter Mell & Timothy Grance (note 63); Bill Williams (note 62).

– **Measured service**: Cloud systems automatically control and optimize use of resources by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both providers and consumers of the utilized service.

Cloud computing services come in several different genres. These broad categories under which cloud-based applications fall are typically called 'service models' and they are the following[65]:

– **Software as a Service (SaaS):** The consumer can use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface (e.g. a Dropbox installation on the user's laptop). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings;
– **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications built using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment;
– **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and

65 Christof Weinhardt, Arun Anandasivam, Benjamin Blau, Nikolay Borissov, Thomas Meinl, Wibke Michalk & Jochen Stößer, *Cloud Computing – A Classification, Business Models, and Research Directions*, 1 Bus. Inf. Syst. Eng. 391–399 (2009); Bill Williams (note 62); Norman Pelzl, Methodische Entwicklung von zukunftsorientierten Geschäftsmodellen im Cloud-Computing, Band 88 (2016.)